Smart Computing In Plain English
REFERENCE SERIES
A Sandhills Publication

Home Networking

MADE EASY

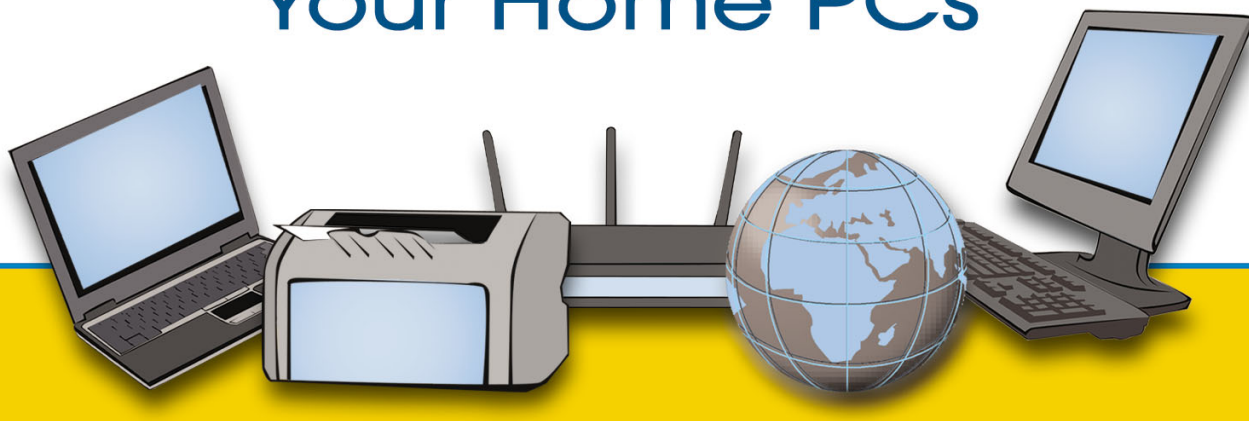
Connect

Your Home PCs

Adding DSL & Cable Connections

Configuring Routers & Firewalls

Setting Up Security & Privacy Options



Adding Wireless Nodes & Extenders

Connecting MP3 Players, DVRs, Printers, Game Consoles & Other Peripherals

Creating Security Setups With WebCams

How To Build & Troubleshoot Wired & Wireless Networks

Covers Powerline, Cable & Wireless Scenarios!

Display Until 11/6/06

Overclock Your Magazine!

Plug into ***Computer Power User*** for all the **latest** and **greatest** in the world of enthusiast-level computing.

CPU
COMPUTER POWER USER
intel
Core 2 Extreme
Intel Core 2 Extreme X6800 (page 21)
SuSE Linux 10.1 & XGL (page 96)
Encoder Roundup: Bend Video Files To Your Will (page 70)
CPU Cooler Comparo: Six Units, No Water (page 17)
INTEL WANTS BACK INSIDE
Smokin' Takes The Checkered Flag (page 36)
Make Your PC Roar With Conroe
THE HOME DEPOT
Q&A with Jerry Bautista
Intel MRL Director On The Future Of CPUs & CPUs (page 108)

- We've got **Modding**
- We've got **Hardware**
- We've got **Reviews**
- We've got **Industry Leaders**

Each month *CPU* brings you a functional mix of hardware reviews, information on modding, the latest and greatest software, and the opinions of some of the industry's leading columnists.

Mike Magee

Alex "Sharky" Ross

Rob "CmdrTaco" Malda

Pete Loshin

Rahul Sood

Anand Lal Shimpi

Barry Brenesal

Chris Pirillo

Alex St. John

Log on to **www.computerpoweruser.com** or call **800.733.3809** to find out how you can try **3 issues**

RISK-FREE! TODAY!

Home Networking *Made Easy*

REFERENCE SERIES VOLUME 10, ISSUE 5

You have two desktop computers, two notebooks, one iPod, one Xbox 360, and one cable modem connection. You want to be able to send print jobs from all four computers to your laser printer in the home office. You want to listen to your iPod through your speakers downstairs and in your living room. You want to play Xbox online from your family room and the kids' playroom. You want to sit on your deck and sip tea on Sunday mornings while you take care of a few business emails to prepare for the coming work week. What you need, of course, is a home network connected to the Internet. Home networks are booming in popularity, driven by the desire to share broadband access, peripherals, and data. Unfortunately, networks can sometimes be complicated to set up and use. Whether you are installing your first network, upgrading, or troubleshooting, the articles in this issue will walk you through the process.

Starting Out

5 **Networking Comes Home**
The Nature Of Networks

8 **What's In A Network?**
Understand How PC Communications Connections Work

11 **The Internet: The Big Kahuna Of Networks**
A Simple Primer On The Biggest Man-Made Thing In The World

14 **Get Wired**
Choosing A Wired Network

18 **Options Aplenty For Wireless Networks**
Choose The Right Wireless Standard For Your Home Or Business

22 **Your Networking Options**
Compare Wires, No-New-Wires & Wireless Networks

Setting Up Networks

24 **Network On The Cheap**
How To Easily Network Two Computers

27 **Getting Wired & Going Wild**
How To Set Up A Wired Network

32 **Wires: Who Needs 'Em?**
How To Install A Wireless Network

37 **Nobody Home?**
Whatever Happened To HomePNA?

38 **A Network In Your Walls**
Install A Powerline Home Network

Special Configurations

41 **Create A Hybrid Network**
Make Your Wireless & Wired Networks Hold Hands

44 **Your Networked Media Center PC**
Entertainment On The Line

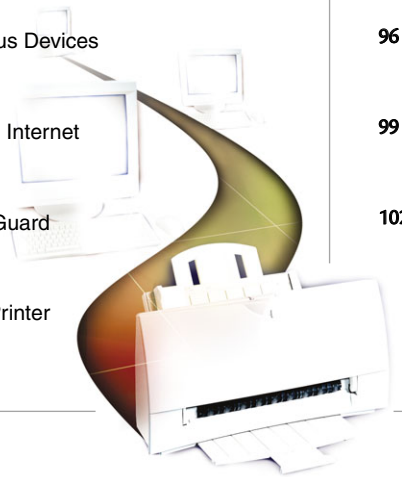
48 **Across The Great Divide**
Combine Macs & PCs On A Single Network

51 **Peripheral Fun**
Networking With Miscellaneous Devices

55 **Gaming Goes Online**
Connect Your Console To The Internet

58 **Home Automation Setups**
Make Your PC Your Security Guard

62 **Print Connections**
How To Install A Networked Printer



Sharing Internet Connections

65 **Share The Bandwidth**
Set Up Internet Connection Sharing On Your PC

68 **How To Share Your DSL Connection**
Advice For A Fast & Easy Setup

71 **Share Your Broadband Internet Access**
Cable Modems Provide Fast Connections

74 **Share A Dial-Up Connection**
Old-School Networking

Networking With Windows

76 **WinXP Networking Wizards & Settings**
Where To Go For Networking Help

81 **Windows 98 Networking Wizards & Settings**
Configure Win98 To Share Folders & Printers

84 **Windows Me Networking Wizards & Settings**
Use Windows Me To Create Your Home Network

87 **Windows 2000 Networking Wizards & Settings**
Go Ahead & Get Connected

Networking On The Road

90 **Sit, Sip & Surf**
Connect Anywhere With Wi-Fi Internet

92 **Configure Your Notebook For Access On The Road**
Get Wireless Internet Wherever You Go

96 **Access Email From Your PDA**
Wherever You Go, Your Inbox Is There

99 **Phoning Home**
Connect To Your PC From The Road

102 **Tunnel Into Your Network With VPN**
Take Your Office
With You

Security & Privacy

106 **Security & Privacy Essentials**
Protect Yourself Online

109 **Protect Your Network**
Keep The Wolves At Bay With A Properly Configured Firewall

112 **Guard Duty**
Choosing & Using Antivirus Protection On A Network

115 **Protect Your PC With Passwords**
Hackers Prey On Computers Without Password Barriers

116 **Setting Up WEP For Wireless Networks**
Shore Up Your Wireless Defenses

118 **WPA Is A-OK**
WPA & WPA2 Security Modes Will Keep You Well-Protected

120 **MAC-Based Security For Wireless Networks**
Secure Your Wireless Network with MAC Address Filtering

122 **Advanced Wireless Security Options**
Protection For SOHO Wireless Networks

Troubleshooting

126 **Troubleshooting Essentials**
Fixes For 19 Common Home Networking Problems

130 **Communication Breakdown**
General Troubleshooting Tips

138 **Wireless Woes**
Fixes For Wireless Network Problems

142 **Networking Snags In Windows XP**
Troubleshooting Tips To Help You Get Up & Running Again

146 **Stay Out Of Trouble**
Solutions For Your Windows 98 Network Problems

149 **Do It Yourself**
Troubleshooting Network Problems In Windows Me

152 **Keep Your Network Happy**
Tips For Fixing Your Windows 2000 Networking Problems

155 **Long-Distance Runaround**
Troubleshooting Remote Access Problems

158 **Networking Glossary**

Online Only

The following material is available on SmartComputing.com as an extra bonus to our readers. You do not need to subscribe to Smart Computing *to read this article; just browse to the address indicated.*

Network Software Tools
Programs That Make Managing Your Home Or Business Network Easier
(www.smartcomputing.com/rs1005/networktools)

Editorial Staff: Ronald D. Kobler / Rod Scher / Sally Curran / Linné Ourada / Corey Russman / Christopher Trumble / Calvin Clinchard / Katie Sommer / Katie Dolan / Raejean Brooks / Michael Sweet / Nate Hoppe / Trista Kunce / Sheila Allen / Joy Martin / Vince Cogley / Ashley Finter / Leah Houchin / Tara Simmons / Marty Sems / Blaine Flamig / Kylee Dickey / Josh Gulick / Andrew Leibman / Jennifer Johnson / Nathan Lake / Holly Zach / Barbara Ball / Sarah Gabelman

Web Staff: Dorene Krausnick / Laura Curry / Kristen Miller

Customer Service: Lana Matic / Lindsay Albers

Subscription Renewals: Connie Beatty / Matt Bolling / Patrick Kean / Charmaine Vondra / Miden Ebert / Kathy DeCoito / Stephanie Contreras / Nicole Buckendahl

Art & Design: Lesa Call / Fred Schneider / Aaron D. Clark / Carrie Benes / Ginger Falldorf / Sonja Warner / Aaron Weston / Lori Garris / Jason Codr / Andria Schultz / Erin Rodriguez / Lindsay Anker

Newsstand: Kelly Richardson

Advertising Sales: Grant Ossenkop / Eric Cobb / Bob Chester

Marketing: Mark Peery / Liz Kohout / Marcy Gunn / Jen Clausen / Scot Banks / Ashley Hannant / Travis Brock / Jeff Ashelford / Ryan Donohue / Brynn Burtwistle

Copyright 2006 by Sandhills Publishing Company. All rights reserved. Reproduction of material appearing in *Smart Computing REFERENCE SERIES: Home Networking Made Easy* is strictly prohibited without written permission. Printed in the U.S.A. GST # 123482788RT0001. *Smart Computing* is published monthly by Sandhills Publishing Company. 131 West Grand Drive, P.O. Box 85380, Lincoln, NE 68501. POSTMASTER: Send address changes to *Smart Computing*, P.O. Box 85380, Lincoln, NE 68501.

Web Services
(For questions about our Web site.)
webhelp@smartcomputing.com
(800) 368-8304

Customer Service
(For questions about your subscription.)
customer.service@smartcomputing.com
Smart Computing
P.O. Box 85380
Lincoln, NE 68501-5308

Hours
Mon. - Fri.: 7a.m. to 8p.m. (CST)
Sat.: 8a.m. to 4p.m. (CST)

To Place An Order Or Change An Address
(800) 733-3809
FAX: (402) 479-2193

Subscription Renewals
(800) 424-7900
FAX: (402) 479-2193
www.smartcomputing.com

Authorization For Reprints
Reprint Management Services
Toll Free: (800) 290-5460
(717) 399-1900 ext. 100
FAX: (717) 399-8900

Editorial Staff
editor@smartcomputing.com
FAX: (402) 479-2104
131 W. Grand Drive
Lincoln, NE 68521

Advertising Staff
(800) 848-1478
120 W. Harvest Dr.
Lincoln, NE 68521
FAX: (402) 479-2193

A Sandhills Publication

Try *PC Today* RISK-FREE!

Subscribe Now at PCToday.com

1 LOG ON TO PCTODAY.COM

2 FILL OUT REQUIRED INFORMATION

3 CLICK SEND ME PC TODAY!

4 ENJOY *PC TODAY* DELIVERED DIRECTLY TO YOU EVERY MONTH.

Questions? Call us at (800)733-3809.

PCT1050

Networking Comes Home

The Nature Of Networks

The computer network is making itself at home in the home. According to Parks Associates, approximately 23 million homes in the United States currently have a household computer network. That number is expected to increase to 41 million by the year 2010. Americans aren't the only ones benefiting, either. The Diffusion Group, taking a global perspective, foresees more than 162 million home networks worldwide within four years.

But who cares what the studies say? Take a look around and you'll find countless home computer users benefiting from personal networks right here and now. They're using them to share broadband Internet access, to swap music files and digital photos, to archive irreplaceable data; in short, to get more value from their computer systems. If you have not yet implemented your own home network, now is certainly a good time to consider doing so.

The Networking Boom

Home networking is nothing new. Among the innovative features presented in Windows 95 when it was released more than a decade ago were several do-it-yourself networking tools that simplified the task of connecting multiple PCs within a home or small office environment. Unfortunately, relatively few users took advantage of these tools. They simply had no compelling reason to do so. Back in the mid-1990s, the Internet was slow, hardware upgrades were a pain in the rear, and few individuals owned more than one computer.

But things changed. The economy boomed, overseas manufacturing plants sprung up faster than you could say "non-union wages," and the price of memory modules, storage drives, circuit boards, and other hardware components took a sharp decline. Suddenly it seemed that anyone could purchase a respectable desktop computer system with all of the requisite perks, such as a CD-ROM drive and dial-up modem, for less than $1,000. Multi-PC households became more common as middle-class users invested in new equipment rather than upgrade what they already had.

Moreover, the cheaper computers were faster and more powerful than their predecessors. Processors could handle video editing and complex gaming algorithms. Hard drives had the capacity to store thousands of audio tracks and digital photos. High-speed USB and Firewire ports made it possible for homeowners to hook up a variety of external devices without knowing a thing about COM ports or IRQ settings.

Oh, and one more thing: Internet access got fast. Gone were the days of dial-up with its harsh screeching and 56 Kbps (kilobits per second) maximum throughput. For about the same price as a cable TV subscription, users could get broadband Internet. The high-speed access options offered around-the-clock connectivity and bandwidth at rates of 1.5 Mbps (megabits per second) or better.

Such changes, occurring together as they did, revolutionized the way people used their home computer systems. Telecommuting became increasingly more popular. The Information Age pushed forward at an astounding pace with computer users generating unprecedented amounts of data, much of it in the form of audio files, digital

snapshots, PDF documents, and archived email. Entertainment options began to orient themselves around the computer, too. A PC could handle the latest shoot 'em-up showdown, for instance, and then double as a jukebox. And, of course, everyone wanted to take advantage of high-speed Internet access.

As the personal computer system matured and evolved, home networks went from being a novelty to a necessity. In addition to linking multiple PCs into a useful peer-to-peer configuration, a network allowed multiple computer users to share a single broadband Internet connection. With a properly configured network, a user in the den could surf the Web for the latest football scores while another user in the bedroom downloaded the hottest singles from Napster. A network also proved useful for sharing access to expensive hardware components. A user who operated a home network could get by with only one printer, scanner, disc burner, and backup drive.

Speaking of backups, a network offered convenient data protection as well. Instead of transferring mission-critical data to removable storage media, users with active home networks could upload the folders and files to another drive on another system. Not only was the data safe there, but it was also immediately available—via the network, of course—if anything happened to the original.

Just Do It

Networks have caught on quickly since the turn of the century. And yet not everyone is convinced. According to studies conducted by research firm Parks Associates, an estimated 37 million homes in the U.S. currently have more than one computer. If only 23 million of these same households have networks, that means at least 14 million multicomputer households are not taking advantage of everything their hardware has to offer.

The fact is users can come up with a variety of reasons for not putting together a home network. The most common reasons are that it's too expensive or too complicated. Both excuses may have been perfectly valid ten years ago, but today they fail to persuade.

Hardware manufacturers trying to get a jump on the next-generation wireless protocol, 802.11n, have begun to release products such as the Wireless-N Broadband Router from Linksys shown here ($149.99; www.linksys.com)—that conform to the expected 802.11n specifications.

The out-of-pocket costs associated with home networking are minimal these days. Users can purchase a consumer-oriented router or gateway from a reputable manufacturer such as Belkin (www.belkin.com), D-Link (www.dlink.com), Linksys (www.linksys.com), or Netgear (www.netgear.com) for less than $50. But even a router may not be necessary. The latest version of Windows XP includes all of the networking software a user needs to set up a small personal network, and most computers now include integrated network adapters, thereby saving users the expense of purchasing—and hassle of installing—a standalone product. As a result, it's possible to set up a simple ad hoc wireless network (see www.microsoft.com/windowsxp/using/networking/expert/bowman_02april08.mspx for details).

Setting up a network is easier than ever, too, thanks to plug-and-play hardware and do-it-yourself tools incorporated into WinXP. The Network Setup Wizard walks users through the process of hooking up multiple computers. Integrated security functionality ensures that the home network is safe from unwanted intruders and nearby bandwidth freeloaders trying to hitch a ride into cyberspace. And so a competent computer user can establish a secure peer-to-peer network in less time than it takes to eat lunch.

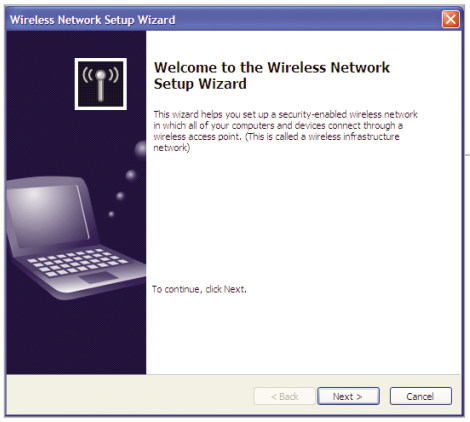
Size Up The Options

Users who decide to take the networking plunge have several decisions to make. The most important decision is whether to invest in a wired or wireless network. Both network types have their unique advantages and disadvantages, although wireless networks have certainly garnered the lion's share of attention in recent years.

Wireless networking. The wireless network phenomenon is quite literally sweeping the nation. Open a wireless-enabled computer in nearly any urban or suburban neighborhood, and odds are good you'll find at least one active network within range. Ditto in thousands of cafes, truck stops, hotels, and malls across the United States. Several major cities, including Houston, Milwaukee, Minneapolis, Philadelphia, and San Francisco, are in the process of deploying comprehensive wireless networks that would be accessible at any location citywide.

The anywhere, anytime presence of wireless Internet access provides a compelling reason to go wireless when setting up a personal network in a home or small office. Another compelling reason to go wireless is that doing so enables users to put up a network without hacking into walls. They can move their computer systems and change the configuration of their offices as often as they want without worrying about how and where they'll plug into the network. They also can accommodate friends and relatives who bring their own computers into a home.

The latest wireless networking hardware generally conforms to the family of 802.11 (also known as Wi-Fi) specifications. The most popular of these specifications is 802.11g, which boasts a maximum theoretical throughput of


Wireless Network Setup Wizard
Welcome to the Wireless Network Setup Wizard
This wizard helps you set up a security-enabled wireless network in which all of your computers and devices connect through a wireless access point. (This is called a wireless infrastructure network)
To continue, click Next.
< Back
Next >
Cancel

The Wireless Network Setup Wizard, which comes with Windows XP Service Pack 2, automates the process of setting up a new wireless network.

54 Mbps and a range that extends 30 feet and beyond. The up-and-coming specification is 802.11n, which promises to double throughput at the very least. Some manufacturers, in anticipation of the protocol's approval in late 2006 or 2007, have released networking devices that conform to the preliminary specifications of 802.11n.

Wired networking. Wireless networking is relatively inexpensive, easy to implement and configure, accessible from any point within its viable range, and wildly popular. Why would a user consider anything else?

Security, for one thing. Any user can bum bandwidth off an unsecured wireless network if he's within range. Cunning hackers outfitted with sniffer software and malicious intents can break in to a wireless network for the purpose of stealing email messages, intercepting passwords, and causing general mayhem. Users who have a vital interest in protecting their data should stick to a wired network armed with antivirus software, antispyware software, and a firewall.

Another benefit afforded by wired networks is speed—the latest Ethernet technologies can transmit data at rates as fast as 1Gbps (gigabit per second)—and reliability. A hardwired connection is not susceptible to interference from microwave ovens, portable phones, and other electronic devices. A hardwired connection will not lose bandwidth to the cheapskate next door who wants to surf the Internet for free by tapping into your wireless network. A hardwired connection delivers a consistent stream of data as long as the wires remain intact.

The most common wired networking option is one involving CAT 5 or CAT 6 twisted-pair wiring and the Ethernet protocol. In a small home or office, users can implement such a network by running loose wires behind large pieces of furniture or tacking them to the shoe molding that runs along the edge of the floor. In larger homes and offices, users typically prefer to install the wiring inside the walls. The demand for home networks has led many home builders and remodelers to install wiring throughout a new home or addition in anticipation of future networking needs. This is referred to as **structured wiring**.

Ethernet is the most common wired networking protocol. It isn't the only one. Other viable options include telephone networks that run through existing phone lines (HomePNA, or the Home Phoneline Networking Alliance), coaxial networks that run through television cables, and powerline networks in which the signal travels through a home's power grid from one electrical outlet to the next (HomePlug, commonly referred to as powerline networking). These alternatives are of most value to those who want to use a home's existing wiring rather than install something new, but tend to be more expensive than traditional wired and wireless networking methods. Also, HomePNA is quickly fading as a home networking option, turning its attention to set-top boxes and other media hardware.

Network Comparisons

Which network is right for you? Check out the strengths and weaknesses of each type of network to see which one has the features you like, and problems you can live with.

Network Type	Pros	Cons
Wireless: 802.11g/n	Access from any point within connectivity range No wiring needed Easy to expand network Very popular	Speed decreases with distance Susceptible to interference Least secure
Wired: Ethernet	Fastest networking option Reliable Most secure	Access from access points only Requires wiring
Wired: cable or phoneline	Fast Reliable Runs on existing wiring	Access from access points only May require new wiring Homeline networking outdated
Wired: powerline	Access from every electrical outlet Easy to expand network	Susceptible to electrical interference Hardware is expensive

Beyond Personal Computing

Twenty years ago, analysts predicted a future in which there would be a PC in every home. That future is nearly upon us. According to Parks Associates, roughly 78 million U.S. homes have at least one PC. As a result, much that we once took for granted has changed. Now the time has come to make a new prediction, one involving a future in which there is a network in every home. And we may not have to wait 20 years for it to come true. RS

BY JEFF DODD

What's In A Network?

Understand How PC Communications Connections Work

A network. It's a term you hear bandied about all the time in computer technology discussions. A network can be as simple as two devices talking to each other or as complex as the entire Internet. There are many types of networks and lots of ways to categorize these networks. We'll discuss what exactly a network is, what software and hardware components make up a network, and what types of networks you might encounter at home or out in the world.

At its most basic, a **network** is the connection of two or more computers (or other devices) for data sharing. These devices can be separated by as little as a few feet or by thousands of miles. Networks can be defined by geographical area (see the sidebar "[X]AN a Do"), by relationships between the networked devices, or by the organization and physical nature of the network.

A Network's Pieces

The best way to understand how a network works is to understand the pieces that make up a network. In a traditional network, there are at least two PCs, but there are usually many more. You can also have other devices that connect to a network, such as PDAs, video game consoles, or cell phones. Any device that connects to a network is called a **node**. Each node will usually have its own network connection and be given a **MAC address**, a Media Access Control number that distinguishes the node from other nodes on the network. The MAC address on your PC is one way that Web sites can identify your PC when you're viewing their pages.

The network connection on a PC is called a **network interface** if it's built into the motherboard or a **NIC** (network interface card) if it's a card that fits into a slot on the motherboard. Both a NIC and a network interface feature a port that looks like a large phone jack that is used for plugging in network cables. This cabling is known as **Cat5 cable**. It looks like a phone cord, but it's thicker with larger plugs on the ends.

Networks can connect at a variety of speeds, but you'll usually find three speeds for network adapters on home computers: 10Mbps (megabits per second), 100Mbps, and the newer 1Gbps (gigabit per second). It takes eight bits to make a byte, so for every eight megabits you transfer, you're transferring one megabyte of data. Most network adapters on PCs are 10/100, which means they can connect to either 10Mbps or 100Mbps networks.

These nodes can be connected to one another directly, but they're usually connected to each other through a central **hub** or **switch** (also known as a **bridge**), boxes that have additional ports for the other ends of those network cables. A hub is more basic than a switch, which gives you more control of the information that runs through it. For larger networks, you will find more complicated "boxes" at the center, such as a router, which eliminate a lot of transmission errors and control the flow of data traffic on a network. See the sidebar "Re-routing" for more information on routers.

Types of Networks

In addition to standard LANs (local-area network), there are other types of home networks including **HomePNA** (Home Phoneline Networking Alliance) that lets you create a

A router connects multiple devices or nodes and then connects that network of nodes to another network.

fast network through your home's telephone jacks and **HomePlug** or PLC (PowerLine Communication) that uses the electrical wires throughout your house to network two or more devices together. You need special hardware to use either of these types of home networks, and most of the major networking vendors offer kits to get you started. And of course, there's the ever-more-popular wireless network that we'll explore in a moment.

If you define networks on how the pieces relate to one another, there are two main classifications: client/server networks and peer-to-peer networks. Client/server networks are more traditional, but P2P (peer-to-peer) networks have grown in popularity in recent years. As you might expect, in a client/server network the **client PC** is the one that the user is on. It makes requests for information from the server PC (or PCs), which stores some type of data that client PCs can access through the network connection. The **server PC** is always "listening" for these requests and then will do its best to quickly provide the information that the client needs.

A good example of a client-server relationship can be seen when you're browsing the Web. Your PC is the client hardware and your Web browser is the client software (in fact, Web browsers used to be commonly known as "clients"). When you type in an address such as www.smartcomputing.com, you are making a request of server hardware and software to transfer the contents of that Web site to your browser so you can view it. (See the article "The Internet: The Big Kahuna Of Networks" on page 11 for more information on the Internet as a network.)

Peer-to-peer networks don't have separate clients and servers. Every node in a P2P network can function as both client and server (although some P2P networks use client/server information exchange for certain tasks such as searching for files). These networks use special software and usually piggyback on an existing network such as the Internet. P2P networks have more specific uses than client/server networks, such as file sharing. Napster was one of the most famous examples of a P2P network that was used to share audio files such as MP3s. Current P2P networks feature the sharing of video files as well, causing them to garner attention (and dismay) from the movie and television industries.

Networks can also sometimes be classified by their **topology**, or the way that they're laid out and how data flows through them. Common topologies are shapes, such as a **ring** or a **star**. In the former, all nodes are connected to two other nodes and the whole network is a circle. A star topology features a central device, such as a hub or a switch, as a common connection for all the nodes on the network. Other network topologies include **bus**, where one cable functions as a backbone for the entire network and **tree**, where there are multiple star networks connected to a bus network. A more complex topology, called **mesh**, incorporates multiple connections between nodes for the routing information and doesn't fit as

[X]AN A Do

This issue focuses mostly on LANs (local-area networks), but there are a variety of other area networks that exist in the connected digital world. Here are the major types of area networks that you might come across.

WAN - Wide-Area Network. Basically the opposite of a local-area network, WANs are used to connect computers over a wide physical area. The Internet is a perfect example of a WAN as it connects computers around the world to one another.

MAN - Metropolitan-Area Network. A small WAN or a big LAN that encompasses a city or a college campus. A MAN usually links several LANs together and may be connected to a WAN that covers several cities or universities.

PAN - Personal-Area Network. A small LAN that covers a single person. A PAN is used for linking smaller devices such as PDAs and cell phones. A Bluetooth wireless network is an example of a PAN. It lets you connect a wireless headset to your cell phone or your PDA to your printer. Some unique clothing items have been created for PANs, such as jackets with cables running through them.

W[X]AN - Wireless WAN, MAN, PAN, LAN, etc. With wireless technologies increasing in power and reducing in cost, there are wireless versions of all of these area networks, from Bluetooth for WPANs to overlapping wireless hotspots across a city for WMANs.

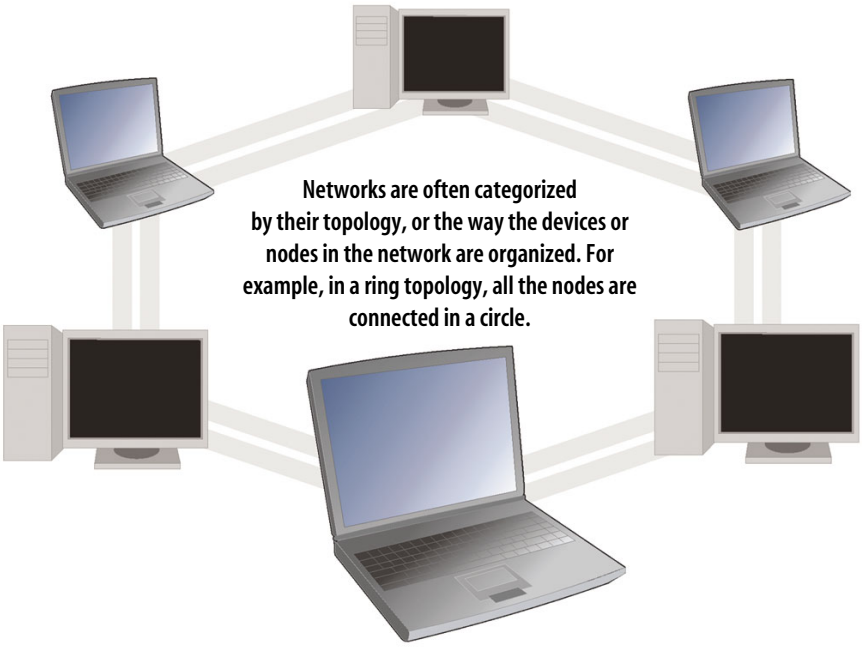
Found In The Ether

Ethernet is actually the more common name of the IEEE 802.3 networking standard. It's the gold standard for local-area networks and is used in almost every company that has a network. The network adapter or NIC (network interface card) found in your PC is often called the Ethernet adapter or Ethernet card.

Ethernet was first developed by Xerox (with a little help from Intel and another company called DEC) in 1976. It has been around in many iterations for many years, and is still going strong. The first Ethernet standard was used in the 1980s and allowed for theoretical speeds up to 10Mbps. This was followed by 100BaseT or FastEthernet that promised speeds of up to 100Mbps. Now Gigabit Ethernet lets networked nodes communicate at up to 1000Mbps. And next up is 10 Gigabit Ethernet, so Ethernet isn't going away anytime soon.

nice a shape as the others (but is a common topology for large networks such as the Internet).

Networks are either wired or wireless. Wireless networks are very popular, with **hotspots** (locations where you can wirelessly connect to the Internet) popping up everywhere from coffee shops to McDonalds. There are many types of wireless networks, such as **Bluetooth**, which lets you connect two devices in close physical proximity to each other, to wireless LANs that connect your home PCs to a wireless router. Home wireless networks have become more common as the costs for wireless hardware have gone down and the technology has improved to the point that an average user can set one up with little trouble. There are still some issues with wireless networks, however, such as interference with other devices and problems with security.



Networks are often categorized by their topology, or the way the devices or nodes in the network are organized. For example, in a ring topology, all the nodes are connected in a circle.

Following Protocol

A network **protocol** is just a fancy way of describing the language a network uses to communicate with devices on the network. One of the most common networking protocols is **TCP/IP** (Transmission Control Protocol/Internet Protocol), two protocols that have been combined to become the language of the Internet. But there are other protocols out there.

Another common protocol is **FTP**, file-transfer protocol. It's still used in many Web sites as a way of moving files from a server to your home PC. When you download a file from the Internet, there's a good chance you're using FTP. Even the letters you use in front of a Web site, "HTTP", stand for a protocol. **Hypertext Transfer Protocol** is the language of the Web and browsers.

Protocols on LANs work in a similar fashion, providing a common language with which all the nodes communicate. With earlier networks, you would have to choose which protocol to use with your node and your network. This was called "binding a protocol" to a device.

For example, many Windows networks in the 1990s, such as those created on Windows 3.11 and Windows 95, used **NetBEUI** (NetBIOS Extended User Interface) as their common language. **Ethernet** is one of the most common LAN protocols used today.

Even wireless networks have a variety of protocols, such as 802.11b or g. In order for your device to communicate on a wireless network, it must support the protocol of that network. For example, you might see "802.11 a/b/g" in the specifications of a PC, meaning it can support all three types of wireless protocols. For more information about wireless networking, see "Wires: Who Needs 'Em?" on page 32.

Understanding networks and how they work doesn't have to be difficult. Once you know some of the lingo that describes them, they can be as easy to comprehend as any other aspect of computing technology. RS

BY JOEL STRAUCH

Re-Routing: Where The Router Fits Into A Network

A router looks like a hub or a switch. It's a box with ports for plugging in network cables. Routers are used for connecting networks together, and they tell the packets of data flowing through the networks where to go by reading the addresses information.

You can use a router to connect your network to the Internet through an ISP (Internet service provider). These routers are often called broadband routers because you'll almost certainly connect your router to a DSL (Digital Subscriber Line) or cable Internet connection. .

Broadband routers can have built-in hardware **firewalls** that protect your home LAN (local-area network) from unwanted outside access. A hardware firewall can afford more protection than a software firewall and can hide the addresses of devices inside the LAN from outside eyes.

As with other networking devices, you can get wired or wireless routers for your home network. Wired routers usually feature four network ports for connecting devices via networking cable, although eight-port (and more) broadband routers are also available. ▌

The Internet: The Big Kahuna Of Networks

A Simple Primer On The Biggest Man-Made Thing In The World

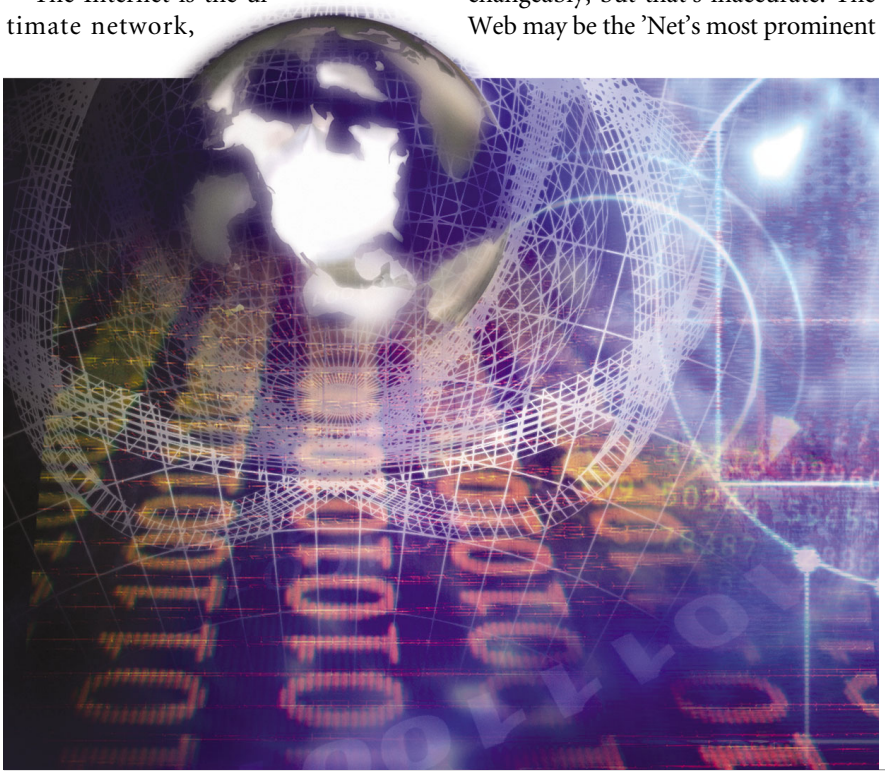
Not to take a turn for the blasphemous, but trying to comprehend the Internet in its entirety is about like trying to understand the mind of God. Getting your brain around something so vast . . . by now, it would probably take a mystic.

But let's give it a whirl anyway. You don't have to know every detail about the 'Net to get a general sense of what makes it tick.

What It Is, What It Isn't

The Internet is the ultimate network, comprising millions of individual networks. These smaller networks belong to colleges, corporations, commercial ventures, and so on. Think of them as separate galaxies within the Internet's universe. They're all interconnected—either physically, with old-fashioned wires or fiber-optic cables, or with wireless signals—and they continually send enormous quantities of data around the world in the blink of an eye.

But what *isn't* the Internet? For one thing, it's not the World Wide Web. Many people use the two terms interchangeably, but that's inaccurate. The Web may be the 'Net's most prominent face—billions of pages with their own unique addresses and often connected by embedded links — but it's still just a subset of the Internet as a whole.



How Do I Access It?

Typically, individual users need an account with an **ISP** (Internet service provider) to access the Internet. This can be an international 'Net-specific company such as EarthLink, a national media outlet such as cable TV company Comcast, a small local provider, and so on. They'll furnish one or more access options for your PC:

Dial-up. This uses your telephone line in the same frequency range as your voice; hence you can't make a call and access the 'Net simultaneously. Although it used to be most users' mode of access, customers are rapidly abandoning dial-up in favor of faster options known as **broadband.**

DSL (Digital Subscriber Line). This high-speed option also uses your phone line, but in a higher frequency spectrum than your voice, so you can talk and surf at the same time. DSL can also be about 50 times faster than dial-up.

Cable. This broadband option piggybacks on cable TV's infrastructure. It's where the greatest potential for even faster speeds lies, as coaxial cable has much more bandwidth capacity than copper telephone lines. Approximately 100 times faster than dial-up, and possibly more.

Other. This catch-all category includes less-used options, including satellite access, wireless Internet options for cell phones and PDAs, etc.

Transactional Analysis

Regardless of how you connect to the Internet, most of what you do will likely conform to a paradigm that involves two components: clients and servers.

A **client** is a computer program that wants something located elsewhere on the Internet. You may have heard your email program referred to as an "email client." Your Web browser is

1 First, you request a Web page by its URL.
2 The Web server sends your Web browser a file coded in HTML.
3 The Browser formats the Web page according to the HTML instructions.

A simplified look at how computers access, download, and display content fro m Web pages. We're omitting the added complexities of DNS and proxy servers.

another client. Also, individual PCs are often referred to as clients (as long as they're not acting as servers).

In order to do what you've instructed it to, a client consults a **server**—another computer or other device (or sometimes just a program installed on the hardware) that stores files and serves them to you upon request. Sort of like your waiter in a restaurant, only without the tipping.

One 'Net, Many Languages

For networks to communicate, they must speak various codified technological languages, known as **protocols**, which determine how data is transferred between devices. A protocol establishes the rules for how a sender signifies that it's sending data and how the recipient signifies message received, as well as the kind of error checking and, if pertinent, the data compression employed.

You can probably guess that something as complex as the Internet utilizes a bunch of protocols. Here are several of the most important:

TCP/IP (Transmission Control Protocol/Internet Protocol). This is the communications backbone of the entire Internet. It actually refers to a group of protocols, the main two of which form the acronym. TCP specifies how computers connect and exchange data streams. IP sets the formatting of the chunks of data (called packets or datagrams) that comprise the data stream, as well as the addressing scheme, so the packets know where to go.

IP Addressing. IP (Internet Protocol) addresses do for the Internet what ZIP codes, street names, and house numbers do for the U.S. Postal Service. Each PC or other component on a network has a unique numerical address to identify it, so other hardware and data can find it. The address format is four numbers (anywhere between 0 and 255) separated by periods. If you have a home network that's not part of the Internet (we don't mean simple Internet service), then you can assign IP addresses however you see fit. But if your network is part of the Internet, with servers for clients to access, you have to obtain registered IP addresses to guarantee that they're unique.

DNS (Domain Name System). As we've just established, locating things

Serving By Proxy

It would be almost impossible for the Internet to function if every request for data or service had to be fulfilled directly. That is, through a direct connection between Point A, the client and Point B, the server.

Instead, networks—and thus the Internet as a whole—rely on components called **proxy servers** to function as intermediaries between clients and primary servers. It's a critical role in the communications process, and without proxies, network traffic might be much slower.

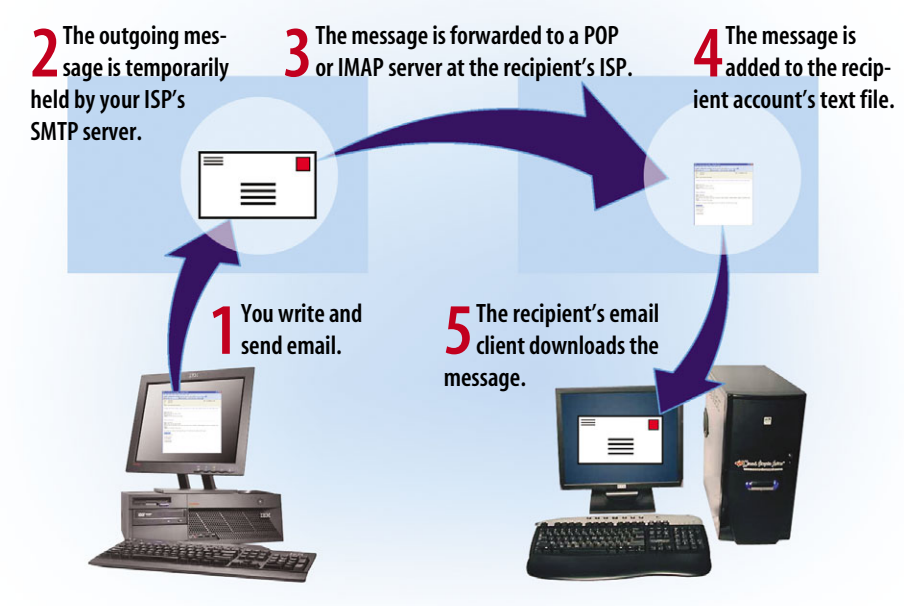
Proxies can be put to many different uses, and one of the main ones is caching.

Let's say that you request data located on a particular network—a Web page, or quarterly reports from a company whose stock you may buy. Your request probably won't go directly to the primary server where this data is stored. Instead, it might go through a proxy server belonging either to the network you're on, or to the same network as the primary server.

The proxy will fulfill your request one of two ways: by connecting with the primary server to get what you need, or by leaving the primary out of it and retrieving your data from a cache stored on the proxy.

How did it get in the cache to begin with? The proxy would've stored a copy when somebody else requested the same data before you did. Caching proxies work best with data that's static—those quarterly reports, for instance. They're of little use for content that's frequently updated, such as blogs.

Proxies can also perform numerous other functions: scanning incoming data for viruses, filtering out content (inappropriate material for school computers, for example), and reformatting Web pages for PDA and cell phone displays, to name a few.


2 The outgoing message is temporarily held by your ISP's SMTP server.
3 The message is forwarded to a POP or IMAP server at the recipient's ISP.
4 The message is added to the recipient account's text file.
1 You write and send email.
5 The recipient's email client downloads the message.

A simplified look at email. We're omitting the added complexities of DNS and proxy servers.

on the Internet is all about numbers. Whereas computers are whizzes at keeping track of long numbers, we humans find words easier to remember . . . Apple and EarthLink and Microsoft, to name a few. In an Internet context, these names are called **domains**, and behind them lies at least one IP address. So, when you want to access a domain's resources, your request requires a DNS server to translate the domain name into its unseen numerical address.

FTP (File Transfer Protocol). This is self-explanatory. FTP covers how files are transferred over the Internet—in particular, how they're uploaded to and downloaded from servers.

HTML (HyperText Markup Language). The coding system used to format the structure of Web pages.

HTTP (HyperText Transfer Protocol). The governing language of the Web, this specifies the formatting and transmission of commands and other messages. HTTPS adds a secure layer to HTTP for encrypted communications such as financial transactions.

POP3 (Post Office Protocol version 3) and IMAP (Internet Message Access Protocol). These dictate the handling of incoming email. IMAP is more complex, and routinely leaves mail on servers for users to access later, or from different computers.

SMTP (Simple Mail Transfer Protocol). The standard protocol for outgoing email.

Greatest Hits

The Internet can be put to many clever uses: gaming among Microsoft Xbox players, relaying emergency medical information, showcasing live collaborations between musicians half a world apart, and many more.

For most people, their normal Internet use comes down to two activities: Web surfing and email. Let's look at how these two essentials work.

Web pages. Every Web page has its own unique address, called a **URL** (uniform resource locater), to make it accessible from any online computer. In addition to specifying the HTTP protocol, the address identifies the domain on whose server the page resides, plus the name of its associated file.

When you access a page, your Web browser first connects with a DNS server to learn the domain's IP address. Your browser then connects to the domain's Web server, requests the file associated with the page, and receives it. This file includes chunks of HTML code called **tags**, which your browser knows how to read, and assembles the page as it's supposed to look. In addition to text, this includes fetching graphics files, audio clips, and other data that are stored on another domain component called an FTP server.

Email. At the heart of email is your email client. Before you can use it, you have to furnish it with such information as your ISP account ID and/or email address, and the ISP's incoming and outgoing mail servers for instance, mail.earthlink.net.

Whenever you write an email message to a friend, it's formatted in simple text and addressed in such a way that it can be routed to the domain that follows the @ symbol, as well as the owner of the account ID that precedes the @, such as editor@smartcomputing.com.

When you send the message, your email client connects to your ISP's outgoing mail (SMTP) server. If you're mailing another user on the same ISP, the message simply gets transferred to the ISP's incoming (POP or IMAP) mail server.

If you're mailing someone on another ISP, however, a few more servers have to get in on the action, such as a DNS server, to translate the domain portion of your friend's email address into an IP address. The message then travels to the POP or IMAP server of your friend's ISP.

The next time he retrieves his mail, his email client connects to his ISP's incoming server and downloads the messages that have accumulated since his previous visit.

Logging Off

If the Internet seems complex, sprawling, and nearly unfathomable, well, it is. But that shouldn't stop you from getting what you want out of it. The important thing is, it works, and amazingly well. And now that you know a little something about how, isn't it all the more impressive? RS

BY BRIAN HODGE

Get Wired

Choosing A Wired Network

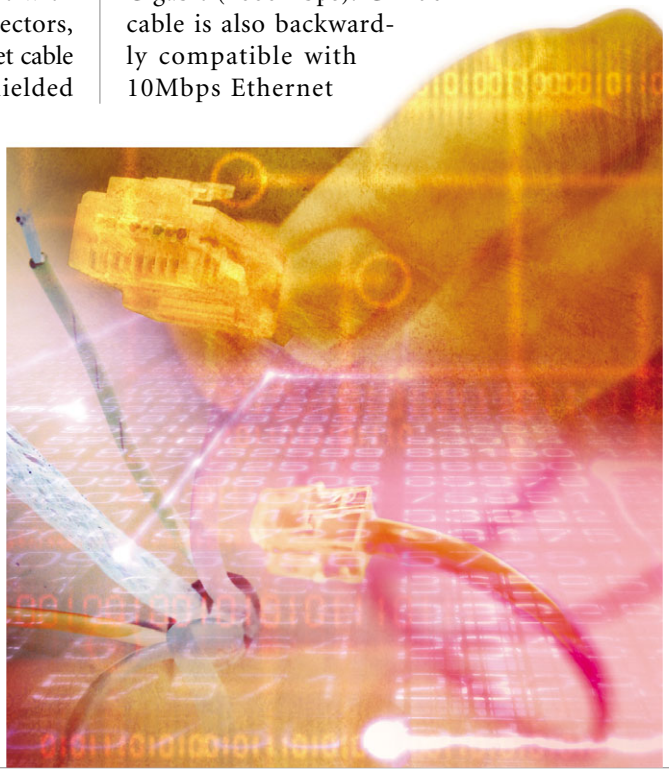
The recent freefall in the price of wireless networking hardware has led some people to argue that wired networks are shuffling off their unshielded mortal coil as a viable networking option. In reality, wired networks offer some big advantages over wireless, including overall speed and security. There also are some types of wired networks that don't require the laying of any new cable, as they take advantage of preexisting wires in your home. If you're thinking about setting up a wired network, here are your main options.

Cable Networks

Cable, or Ethernet, is by far the most common of all the wired networking options. Ethernet cable resembles traditional phone cabling, albeit with thicker wires and larger connectors, called RJ-45 connectors. Ethernet cable is also known as UTP (unshielded twisted pair) cable, namely because the unshielded insulated copper wires of the cable are twisted to reduce electromagnetic interference. The lack of shielding makes the wires more flexible and cheaper to produce. A typical Ethernet cable has eight color-coded wires twisted and aligned in the RJ-45 plug according to TIA/EIA (Telecommunications Industry Association/Electrical Industries Association) standards.

The arrangement of the twisted wires in the RJ-45 plugs differs between crossover and patch cable. The two RJ-45 plugs of an Ethernet patch cable are identical, while the RJ-45 plugs of an Ethernet crossover cable feature a pair of reversed wires. (**Crossover cable** is useful for connecting two computers together without a hub. **Patch cable** is necessary for connecting two or more computers to a hub, router, or switch.)

Ethernet cables also come in a variety of classes, or categories. Of the categories you're likely to encounter, Category 5, or CAT5, is probably the most common. You can use CAT5 cable for 10BASE-T (10Mbps [megabits per second]) networks, and 100BASE-T (100Mbps) Fast Ethernet networks. Category 5e, or CAT5e, features improved insulation and is better suited to higher-throughput networking, such as 1000BASE-T, or Gigabit (1000Mbps). CAT5e cable is also backwardly compatible with 10Mbps Ethernet equipment. Category 6, or CAT6, is an even stricter standard designed for Gigabit networking. CAT6 cable is even less susceptible to unwanted interference than CAT5 and CAT5e.



Installing a cable network with two or more computers consists of running Ethernet patch cable between the network adapter ports of your computers and a central networking device, such as a hub, router, or switch. This central device manages the incoming and outgoing data to make sure it gets where it needs to go. For more information on installing a wired cable network, see "Getting Wired & Going Wild" on page 27. If you're just wiring two computers together, you can forgo the central networking device and just use a crossover cable. We'll describe crossover cable below, but for information on how to create a two-PC-file-sharing network using crossover cable, see "Network On The Cheap" on page 24. For more information on the cost of implementing an Ethernet network, see the "What I Need & What It Will Cost Me" sidebar.

Although wireless networks are noted for their distinct lack of wires, if you are upgrading your network to use an external wireless router, you may still need a length of Ethernet cable to span between your wireless router and the main computer's network adapter. For more information about creating a wireless network see "Wires: Who Needs 'Em?" on page 32.

Phoneline Networks

You're probably aware that you can patch in for dialup or broadband DSL (Digital Subscriber Line) Internet service using the phone lines that connect your home or business to

the phone company's central switching office or PBX (Private Branch Exchange). But inside your home or office, those copper phone lines can also be used to network your computers together.

The key to phoneline networks is in a technology called FDM (Frequency-Division Multiplexing), which lets your copper phone line carry multiple data and voice channels simultaneously as a series of alternating frequencies. This is how your computers can maintain their phoneline network connection even if you decide to take or make a phone call.

A consortium of more than 150 companies formed the HomePNA (Home Phoneline Networking Alliance) years ago to develop and promote phoneline networking standards, also called HPNA. For the sake of clarity, we'll refer to the organization as HomePNA and the standards themselves as HPNA. HomePNA member companies include 3Com, Agere Systems, AMD (Advanced Micro Devices), AT&T Wireless Services, and Motorola.

In 1998, the Alliance released the initial standard, HPNA 1.0, capable of data transmission speeds of up to 1Mbps. Soon afterward, the Alliance updated the specification in its HPNA 1.1 revision, but only improved the protocol's resistance to interference. The early versions of HPNA technology couldn't support high-bandwidth home networking applications, such as gaming and streaming media, which limited their appeal.

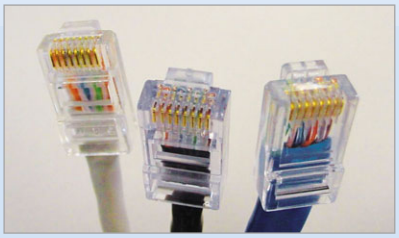
With the arrival of HPNA 2.0 in September 2000, phoneline networking achieved a 10Mbps throughput rate at a distance of up to 1,000 feet, which is comparable to 10BASE-T Ethernet networks. The standard is also backwardly compatible with HPNA 1.0 and 1.1 equipment. In 2002, the Alliance released the HPNA 3.0 standard, which supports faster than Fast Ethernet speeds at 128Mbps and Quality-of-Service (an uptime and bandwidth reliability guarantee). HPNA 3.0 is also backwardly compatible with previous HPNA standard-based equipment. As we went to press, the HomePNA was hard at work on a 3.1 revision of its phoneline networking protocol, which aims to increase throughput rates to support IPTV (Internet Protocol Television), HDTV streaming, and other bandwidth-hungry applications.

Despite HomePNA's best efforts, however, customers have been slow to rally to phoneline networking. In recent years the main attraction for this type of network—avoiding the need to install new wires—has been co-opted by wireless networking standards, and today there are few manufacturers of HomePNA-based hardware.

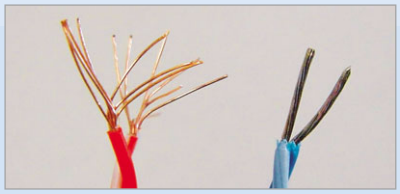
Still, installing a phoneline network is possible, as long as your home or business is less than 10,000 square feet and your current phone wiring is capable of carrying a voice signal. Don't be fooled into thinking

Cabling Connections

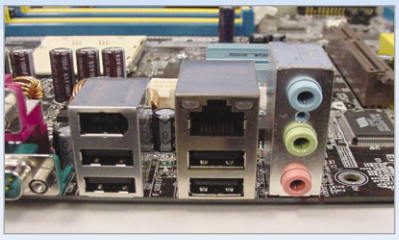
If you're a wired-networking newbie, you should familiarize yourself with the various cable types, jacks, plugs, and ports before taking the plunge.



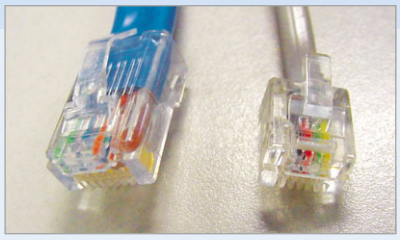
CAT5, CAT5e, and CAT6 Ethernet cables all feature the same RJ-45 plugs and look identical on the surface. For this reason, make sure you check the label stamped on the wire sheath.



The difference between CAT5 and CAT5e cables isn't noticeable even when you remove the plastic wire coating. CAT5 (left) and CAT6 (right) cables are very different, however, with the CAT6 conductors composed of a thicker gauge wire.



This motherboard has an integrated network adapter into which you can plug the RJ-45 jacks of your Ethernet cable.



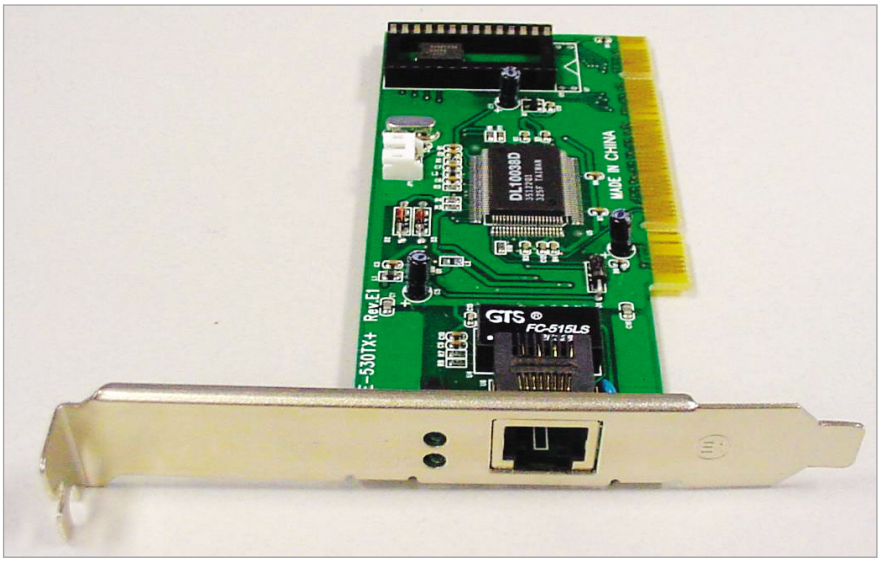
The RJ-45 plug on the left is used in cable networks and the RJ-11 phone plug on the right is used in phoneline networks.

This external phoneline network adapter features an RJ-11 port and a USB plug.

This powerline network adapter plugs into a regular wall outlet and connects to your computer with a USB cable.

that the RJ-11 (phone plug) port on your computer's fax modem will let you use it as a phoneline network adapter. To create a phoneline network, each computer you want networked will require either an external (USB) or internal (PCI [Peripheral Component Interconnect]) phoneline network adapter. A phone line-capable gateway or router might also be necessary to connect each computer to the Internet. Or you can setup ICS (Internet Connection Sharing). For more information on ICS, see "Share The Bandwidth" on page 65.

For the costs involved in setting up a phone line network, check out the "What I Need & What It Will Cost Me" sidebar. For more information on the current state of phone line networks, see "Nobody Home?" on page 37.



A Network Interface Card like this fits into a PCI (Peripheral Component Interconnect) slot on your computer's motherboard.

Powerline Networks

Powerline networking, the other no-new-wires alternative, is designed to transmit data through your home's existing power infrastructure, from outlet to outlet. This means that a powerline system lets you network any room in your home or business that has a power outlet, without having to install additional cabling. Unlike HomePNA networks, powerline networks have gained more traction in the marketplace, and there are more products readily available at retail outlets that support this standard.

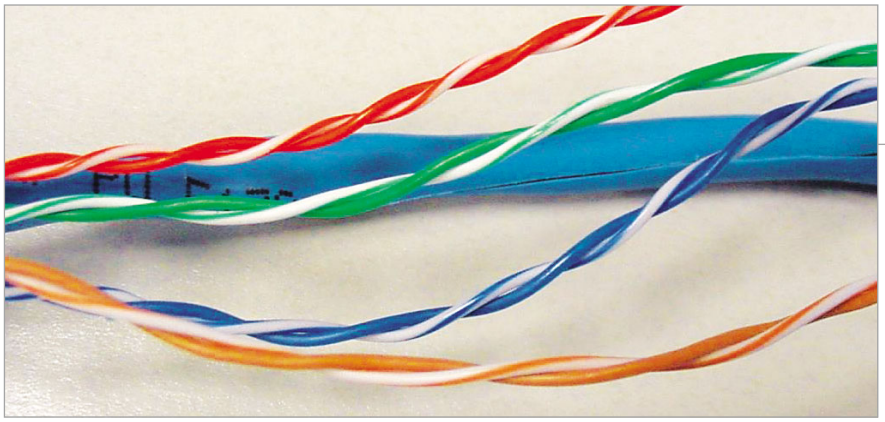
A powerline adapter lets you build a network without laying new wires.

Powerline networks employ a form of Frequency Division Multiplexing, similar to that used in phoneline networks. An integrated chip in powerline networking equipment uses OFDM (Orthogonal Frequency-Division Multiplexing) to generate multiple channels, or carriers, for transmitting the data while maintaining a very steady stream of power to your electronic devices. Current powerline technologies also make use of something called forward error-correction, which helps to ensure that a power surge or other interference doesn't interrupt the data flow.

Since the early eighties, multiple organizations have formed industry alliances in an attempt to hammer out a standard for equipping traditional power lines with data-carrying capabilities. The early standards, such as X-10, CEBus (Consumer Electronics Bus), and LONworks (Local Operating Networks) were primarily concerned with home and business automation.

More recently, the HomePlug Powerline Alliance (with members such as Intel, Linksys/Cisco, Samsung, and Sony) has developed the HomePlug and HomePlug AV standards for networking two or more computers together.

The HomePlug Powerline Alliance introduced the HomePlug 1.0 networking standard in 2001. This initial standard is capable of transmitting data through your home or business at up to 14Mbps, which is ideal for sharing an Internet connection and transporting small and medium-sized files between your networked computers. In addition to the security of a wired network, HomePlug 1.0 employs an encryption password to protect your data. Currently, you can find a range of HomePlug 1.0 equipment for sale. For more information on pricing,



The wires inside Ethernet cable are twisted to reduce interference.

see the "What I Need & What It Will Cost Me" sidebar.

In 2005, the HomePlug Powerline Alliance's consumer electronics manufacturers finalized the HomePlug AV standard, which is designed to handle the demands of HDTV, VoIP (Voice over Internet Protocol), and Home Theater applications. HomePlug AV supports high-speed data throughputs of between 100 and 200Mbps. HomePlug AV also features secure connectivity and Quality-of-Service, or a guarantee of stable uptime and bandwidth. Leading manufacturers of HomePlug AV equipment include Arkados, Aztech Systems, GigaFast, Intellon, and ST&T Corporation. This technology only recently became a standard, and according to the HomePlug Powerline Alliance, you should be able to purchase HomePlug AV equipment by the end of this year.

Another up and coming powerline technology is called BPL (Broadband over Power Line), which is designed to allow your local power utility to provide Internet access over the power lines. In the past few years, the adoption of BPL has been somewhat limited to Europe and a handful of markets in the United States, including Cincinnati, Ohio; Manassas, Va.; New York City; Detroit; and Washington, D.C. For most utilities, installing BPL equipment was fairly expensive and the early revisions of the technology interfered with short-wave and emergency radio frequencies. As the technology has matured however, these problems have been significantly reduced or eliminated altogether with the help of FCC (Federal Communications Commission) regulations. The HomePlug Alliance is currently working on its HomePlug Access BPL standard, which hopes to speed the adoption rate of BPL. If it's successful, ISPs (Internet service providers) such as telcos and cable operators could have a new competitor in the form of your local power company. For detailed instruction on how to install and configure a powerline network, see "A Network In Your Walls" on page 38. RS

BY ANDREW LEIBMAN

What I Need & What It Will Cost Me

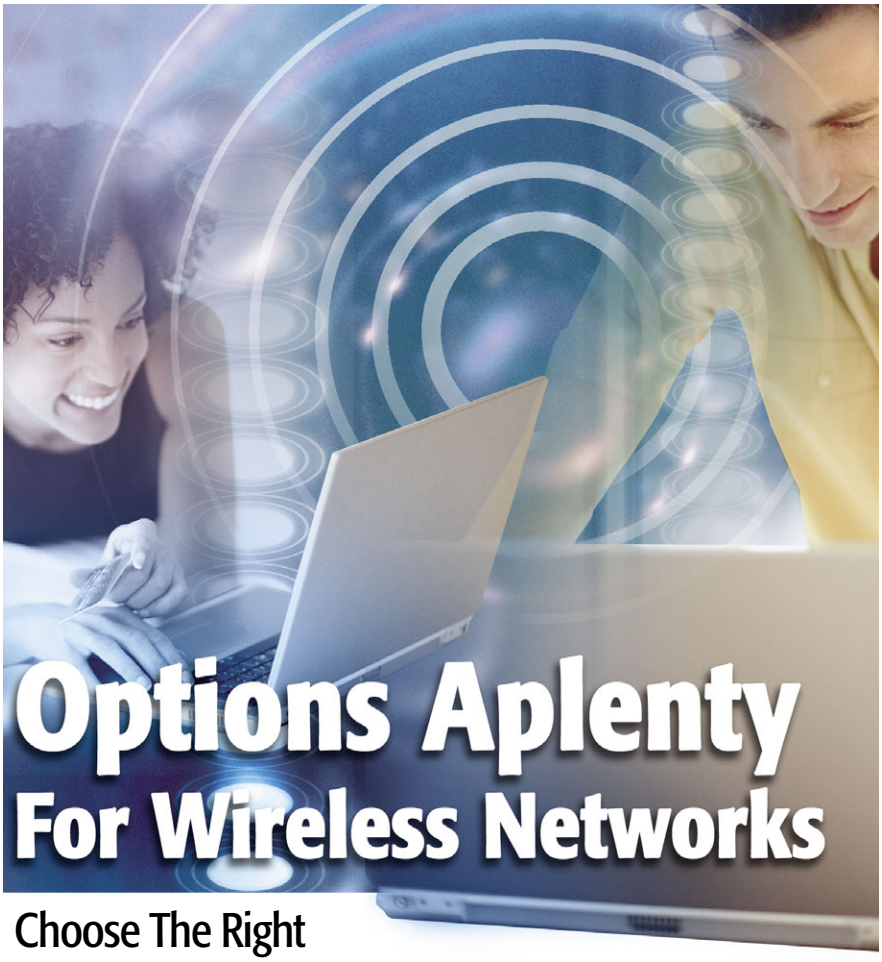
Setting up a wired network is a practical task that can vastly improve your computing experience. Let's say, for instance, you have a main computer in the den, another computer in your office, and a third computer in your daughter's room. Connecting them all together can net big results for not a lot of investment.

Cable. In this scenario, we'll assume your main computer came with a NIC (network interface card), but the computers in your office and your daughter's room each need a NIC. You can find two Airnet 10/100Mbps (megabits per second) NICs for $4 each at NewEgg (newegg.com). You can also pick up a 4-Port Netgear 10/100Mbps hub for $35, and three 15-foot lengths of CAT5e Ethernet cable for $4 apiece. Each item has a shipping charge of $5, making your total purchase price less than $85 after shipping.

Phoneline. To set up a phoneline network using the same scenario, you can purchase three external USB HomePNA 2.0 network adapters from 2Wire for $13 each, with free shipping from JustDeals (justdeals.com). You can get three 14-foot lengths of silver satin wiring (phone cable) for $3 each from TigerDirect (tigerdirect.com). Your total out-of-pocket expenses for this phoneline network amount to $48, making it the budget buyer's best choice.

Powerline. To install a powerline network in this scenario, you can purchase three external NovaTech powerline USB adapters for $21 each from NewEgg (free shipping). To complete the connection, you can get three generic 3-foot lengths of USB cable from NewEgg for $1.30 each, plus a $5 shipping charge, bringing the total cost for this powerline network up to $82.

NOTE: For more information comparing wired and wireless networking standards, see "Your Networking Options" on page 22.



Options Aplenty For Wireless Networks

Choose The Right Wireless Standard For Your Home Or Business

It's a great time to go wireless. With name-brand routers hovering in the $50 range, it's difficult to justify staying on a wired network with all the benefits you get from cutting the cord. Virtually all laptops made in the past several years include built-in wireless cards. You can upgrade desktop computers using a wireless USB adapter without even having to open them. It's both easy and inexpensive to connect multiple computers around your home or business wirelessly, and to share a single Internet connection between them.

However, deciding on the right kind of wireless networking equipment isn't always so simple. The Institute of Electrical and Electronics Engineers (IEEE, often pronounced I-triple-E) first ratified the original 802.11 specification back in 1997. As time went on, the IEEE ratified several newer standards. With these new standards came faster speeds, greater range, better security, and (in some cases) less interference between different networks and other devices that use the same frequency band.

Unfortunately, multiple standards can cause considerable confusion in the marketplace. Let's say you're shopping for a new wireless router. Do you buy an 802.11g device, or one of the latest Draft N products? Do older 802.11b devices still work? What about the range: will a single router cover your whole house or place of business? Can you connect your printer wirelessly as well, or do you still need to tether it to one of the computers?

This article aims to demystify the four most common wireless standards: 802.11a, 802.11b, 802.11g, and 802.11n (or "Draft N," the currently available version of the *n* standard). We'll compare their speed, range, security, and flexibility, and in the sidebar entitled "What I Need & What It Will Cost Me," we'll go over a typical home network setup.

Before we get started, there's one important caveat: speeds tend to drop as you move farther from the wireless router. In an ideal setting such as a large open space, you might be able to travel hundreds of feet in any direction from the router before you start to see serious speed degradation. However, sheetrock, external walls, cabinets, floors, and ceilings can interfere with signals and greatly cut the available range.

It's not uncommon for someone in a 30 x 50 foot house to run into connectivity problems if they only have one router, especially if they're on a different floor from where the router is located. This is why greater range capability is important, even though you might not have any plans to travel 300 feet or more from your router.

The First Widespread Wireless Standard: IEEE 802.11b

The 802.11b standard is the one that put wireless networking on the map for many computer users. The IEEE ratified 802.11b in 1999, and products began to appear on the market almost immediately afterwards. One popular example, the original Apple AirPort router, debuted in July 1999.

You can find 802.11b compatibility in virtually all wireless networking products sold to date, with the notable exception of 802.11a-only devices (see below). 802.11b operates on the 2.4GHz frequency band, which means it can interfere with 2.4GHz cordless phones, some microwaves, baby monitors, and even some Bluetooth devices. Although speeds top out at a theoretical 11Mbps, most of the time you'll see transfer speeds around 6Mbps. That's generally fast enough to surf the Web from a DSL or cable connection, but fairly sluggish for large file transfers, and downright too slow to stream video.

One positive aspect of 802.11b is its range. In typical use you can expect to use 802.11b up to about 100 feet away from a router or access point without serious speed degradation. 802.11b offers a maximum theoretical range of 300 feet, though as you approach that range, speeds will decrease considerably. When they were first released, 802.11b products often included weak security. Usually the best you'd find is WEP (Wired Equivalent Privacy), which can keep out garden variety intruders but is no match for anyone who is serious about breaking into your computer network.

Should you purchase 802.11b-only products? At this point it's safe to say no. You may even have a tough time even finding any in some stores. Newer 802.11g products generally are inexpensive, include 802.11b compatibility, and are much faster. Few devices at this point work with 802.11b exclusively, so it's essentially a non-issue, but it's good to know about it in case you ever want to connect an older device to your network.

The Business Network Alternative: IEEE 802.11a

Many people remember 802.11b as being the first widespread wireless networking standard (disregarding the original 802.11, or "legacy" specification, which was limited to 2Mbps). However, in 1999 both 802.11a and 802.11b were ratified, though it took a couple of extra years before any 802.11a products hit the market.

Designed mainly for business applications, the two main advantages to 802.11a are its speed and the frequency at which it operates. Products based on 802.11a are capable of reaching speeds up to 54Mbps, which is much faster than 802.11b. Real world speeds hover above 20Mbps. However, 802.11a devices communicate faster at the expense of range. Most 802.11a products generally work only in the same room, with a theoretical maximum up to about 60 feet.

As for frequency, 802.11a products operate on a different band: 5GHz. This band is more tightly regulated than the commonly used 2.4GHz frequency, so you're less likely to experience interference with other devices. However, while *b*, *g*, and *n* products can all mix freely on the same network, 802.11a products can only talk to each other. If you're setting up an 802.11a network, every single piece on the network needs to have 802.11a compatibility.

The NETGEAR RangeMax Next Wireless Router – Gigabit Edition, Model WNR854T ($169, www.netgear.com) supports Draft N with advanced MIMO technology.

Popular PC and laptop manufacturers like Dell offer easy and inexpensive upgrades to support 802.11a. However, these upgrades are generally not necessary. If you set up an 802.11a network, you'll lock yourself out of the ability to use a lot of devices that only work on 802.11b and *g* networks, such as home security cameras and the majority of wireless USB print servers. To make matters worse, if a friend or colleague brings over a laptop, that machine likely won't have 802.11a capability, and your friend won't be able to log onto your network. At this point, the only reason to purchase an 802.11a product would be if you or your workplace already has an existing significant investment in 802.11a technology.

Today's Most Popular Choice: IEEE 802.11g

The newer 802.11g standard (ratified in 2003) offers most of the advantages of 802.11a, but without the compatibility and range issues. Most laptops, network cards, routers, and other Wi-Fi devices (such as standalone VoIP—Voice over Internet Protocol—phones) sold in the past two to three years support this standard. You can reach average, real-life speeds in excess of 20Mbps, about

What I Need & What It Will Cost Me

Popular vendors for 802.11g include Belkin, D-Link, Linksys, NETGEAR, and USRobotics. For Draft N, Belkin, Linksys, and NETGEAR all have good options, and D-Link just recently joined the fray with two draft-N routers. USRobotics is sitting out this round, preferring to wait until we're closer to a proper 802.11n standard.

Let's look at a basic wireless network with one router, two desktops, and one laptop computer. Here's what you will need:

802.11g:	
Router	($59 to $79)
One PC card	($49)
Two PCI cards	($69 x 2)
Estimated Total:	$246 to $266

Draft N:	
Router	($129 to $149)
One PC card	($99 to $119)
Two PCI cards	($99 to $119 x 2)
Estimated Total:	$426 to $506

three times what you'd see on a regular basis with 802.11b; it even has the same theoretical maximum (54Mbps) as 802.11a.

All 802.11g devices use the same 2.4GHz frequency as 802.11b. In addition, 802.11g networks can support products that only use the older standard, though network performance will slow down whenever an 802.11b device joins the network. The same interference problems that occur with 802.11b can also occur with 802.11g. Some people find that they have to purchase a new cordless phone, or relocate their old one, when setting up an 802.11g network.

One advantage of 802.11g over the older 802.11a and 802.11b standards is increased security in the form of WPA (Wi-Fi Protected Access) encryption. While 802.11g itself didn't explicitly include the new security standard, WPA encryption was ratified in early 2004, right around the time that 802.11g products became commonplace. As a result, many products that support 802.11g also include support for WPA encryption. WPA is vastly superior to the easily crackable WEP encryption found in many older 802.11b-only devices.

So what's the downside to 802.11g? Aside from interference issues, there really isn't one, unless you're looking for very high speeds. 802.11g is fast enough to take advantage of broadband connections, and does the job well (though not spectacularly) when streaming media. It's fine for streaming both audio and video, but don't expect

Hardware Components

Modem: Your cable or DSL broadband provider gives you a modem when you sign up for service. This is the device that transmits data to and from the Internet. If there's only one computer and no network in place, you'd connect your computer directly to the modem with a single cable.

Router: This is the heart of your wireless network. It enables you to share an Internet connection among multiple PCs and also lets those PCs talk to each other. At this point it's more practical to purchase either an 802.11g router, which is inexpensive and reasonably fast, or an 802.11 Draft N router, which is much faster and has greater range, but also has potential compatibility issues between different brands of networking products.

Wired Desktop: Most wireless routers come with at least one Ethernet port (and often four or more) for connecting computers with an Ethernet cable. This is still faster than both 802.11b and 802.11g, though Draft N products can rival the performance of wired 100Mbps Ethernet. If your main PC is located close to your modem and router, you can use a wired connection and save the cost of purchasing a wireless network adapter for that machine.

Wireless Desktop: Any desktop PC with a wireless PCI card or USB adapter can connect to the network wirelessly. If you're buying a Draft N router, we recommend you get a Draft N PCI or USB adapter from the same brand that's designed to match up with the router.

Wireless Notebook: Nearly all laptops sold since 2003 have a wireless card built-in. This wireless card usually supports both 802.11g and the older 802.11b standard. If you're buying an 802.11g router and you have a recent laptop, you're all set. If you have an older laptop, or if you're purchasing a newer Draft N router, you'll likely need to upgrade your laptop's wireless capability. In this case, look for either a PC card or a small USB network adapter.

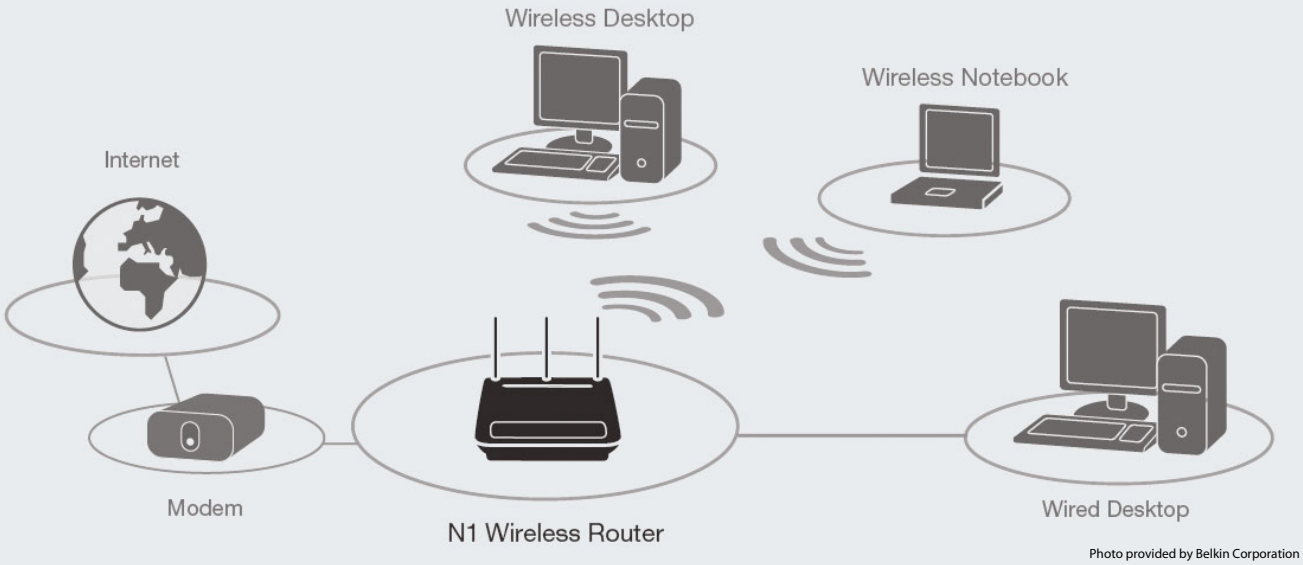
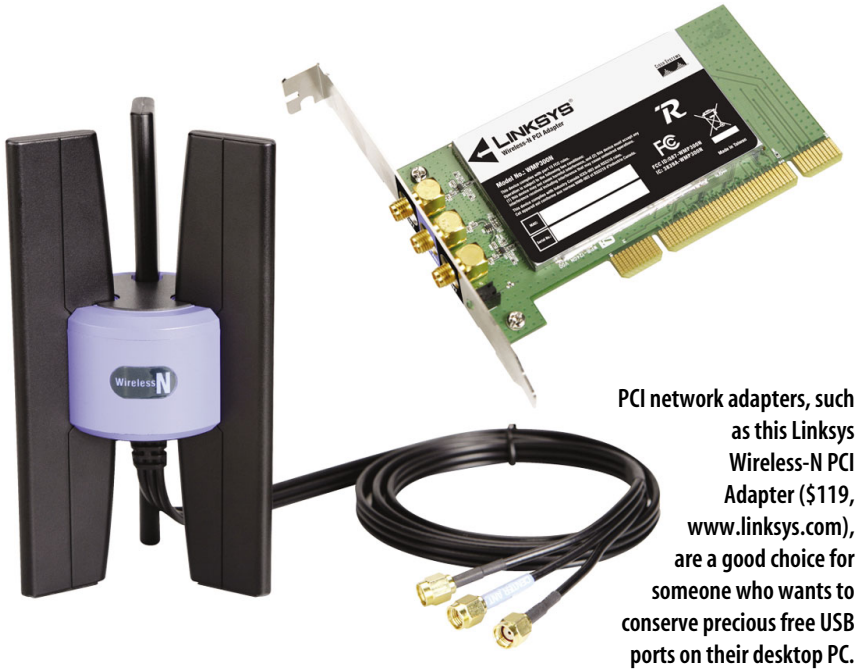


Photo provided by Belkin Corporation



PCI network adapters, such as this Linksys Wireless-N PCI Adapter ($119, www.linksys.com), are a good choice for someone who wants to conserve precious free USB ports on their desktop PC.

to stream HD-quality video wirelessly over an 802.11g network; for that you'll need to move up to 802.11n.

You may have noticed a subcategory of 802.11g products that has appeared recently. Some vendors introduced product lines that increase the speed of 802.11g using their own proprietary enhancements. An example of this type of product is the Linksys Wireless Router with SpeedBooster (WRT54GS). These types of products can be a good choice, providing that you also purchase compatible network cards for each machine that support the same enhancements. If you have a laptop with a built-in 802.11g card, and you connect it to the above router, you won't see any speed improvement. But if you install the Linksys Wireless Notebook Adapter (WPC54GS) in that same laptop, you'll be able to take advantage of higher speeds.

The Future, With Some Options Available Today: IEEE 802.11n

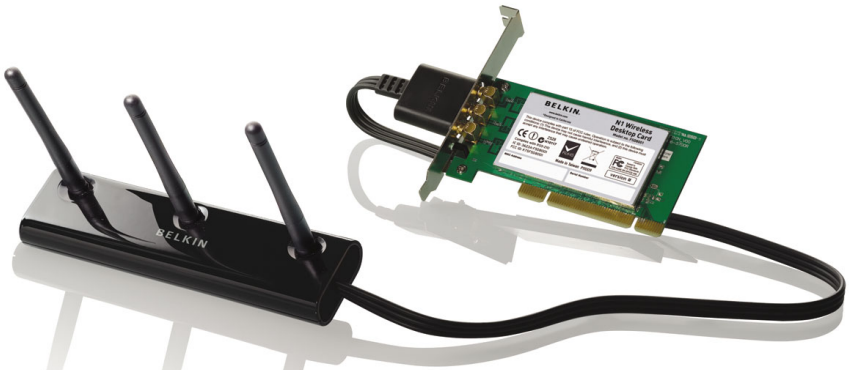
Here's where things get a little complicated. The coming 802.11n standard promises a number of exciting new features, including speeds over 10 times as fast as 802.11g, and nearly quadruple the range, often extending out past 1,000 feet. 802.11n also offers full compatibility with *b* and *g* products, plus stronger interference rejection, even though it's on the same frequency band as the other two networks.

The key characteristic of 802.11n is MIMO (Multiple In/Multiple Out) technology. This enables 802.11n routers to use several antennas for multiple simultaneous signals. The routers are also capable of switching between different channels automatically in order to eliminate or reduce any nearby interference. Other enhancements include channels with nearly double the bandwidth as 802.11g.

While the official 802.11n standard won't be ratified until sometime in 2007, many products have already appeared on the market. Last year we saw a slew of "Pre-N" routers and adapters; now we're seeing a new bevy of devices based on the "Draft N" standard, which incorporates numerous improvements. Examples include the Belkin N1 Wireless Router and the Linksys Wireless-N Gigabit Router with Storage Link (WRT350N).

Theoretically, the Draft N products available today are close to whatever the final standard ends up. Most likely they will be upgradeable via a firmware update to match the new standard when it's ratified. However, this isn't guaranteed. There's a small but real possibility that the final 802.11n specification will differ significantly enough that it won't work with the Draft N products available today. Moreover, we've heard numerous reports of interoperability problems between Draft N products from different vendors.

Admittedly, Draft N is the fastest wireless networking technology and gives the best range. If it was our money, we'd still stick with 802.11g and let the market shake itself out. But if you're bent on staying on the bleeding edge, we strongly recommend you purchase all Draft N products from the same brand, and even the same product line. RS



While 802.11g PCI adapters often included a small foldable antenna, Draft N products such as this Belkin N1 Wireless Desktop Card ($119, www.belkin.com) include a slightly bulkier series of MIMO antennas.

BY JAMIE LENDINO

Your Networking Options

Compare Wires, No-New-Wires & Wireless Networks

	Type	Peak Speed	Interface	Media	Distance	Security
WIRED	Ethernet (802.3/10BaseT)	10Mbps (megabits per second)	RJ-45	CAT5/5e/6 Ethernet cable	994 feet	No built-in security
	Fast Ethernet (802.3u/100BaseTX)	100Mbps	RJ-45	CAT5e/6 Ethernet cable	328 feet	No built-in security
	Gigabit Ethernet (802.3z/1000BaseT)	1000Mbps	RJ-45	CAT5e/6 Ethernet cable	328 feet	No built-in security
	10 Gigabit Ethernet (802.3ae)	10,000Mbps	FC, FDDI, LC, MT Array, SC, SC Duplex, or ST	fiber optic cables	25 miles or more	No built-in security
	HomePNA 1.0	1Mbps	RJ-11, coaxial	silver satin wiring (phone cable), coax	492 feet	No built-in security
	HomePNA 1.1	1Mbps	RJ-11, coaxial	silver satin wiring (phone cable), coax	492 feet	No built-in security
	HomePNA 2.0	10Mbps	RJ-11, coaxial	silver satin wiring (phone cable), coax	994 feet	No built-in security
	HomePNA 3.0	240Mbps	RJ-11, coaxial	silver satin wiring (phone cable), coax	994 feet	No built-in security
	HomePNA 3.1	320Mbps	RJ-11, coaxial	silver satin wiring (phone cable), coax	N/A	No built-in security
	HomePlug 1.0	14Mbps	power plug	4.5 to 21MHz frequency range	654 feet	Password protected hardware, built-in encryption
	HomePlug AV	200Mbps	power plug	4.5 to 21MHz frequency range	654 feet	Password protected hardware, built-in encryption
WIRELESS	802.11b	11Mbps	antenna	2.4GHz radio band	300 feet	WEP (Wired Equivalent Privacy), WPA (Wi-Fi Protected Access)
	802.11a	54Mbps	antenna	5GHz radio band	150 feet	WEP, WPA
	802.11g	54Mbps	antenna	2.4GHz radio band	300 feet	WEP, WPA
	802.11n	100Mbps and up	antenna	2.4Ghz and 5GHz radio band	N/A	WEP, WPA

Networking Comparison Chart

No single networking technology is ideal for everybody. Choosing the right option can depend on your budget, your existing infrastructure, the reasons you want to build a network, the structural limitations, and about a dozen other factors that only you can determine. It's important to know the basics when making this decision and this chart aims to help you understand the main networking technologies from which you can choose.

The Cost Per Node and Setup Time data is based on the costs and time involved in building a three-node network. Data that was unavailable or not applicable is labeled as N/A. RS

BY ANDREW LEIBMAN

Advantages	Disadvantages	NIC* Prices	Router Prices	Misc. Prices	Cost Per Node	Setup Time
Fast enough for Internet and limited file sharing, affordable	Limited range, slow, requires physical wiring	$12	$22	$15 (cabling)	$25	4 hours
Fast enough for most applications, backward compatible with 10Mbps equipment	Limited range, requires physical wiring	$15	$30	$15 (cabling)	$30	4 hours
High-throughput, backward compatible with 10/100Mbps equipment	Limited range, requires physical wiring	$15	$50	$15 (cabling)	$37	4 hours
Ultra-high throughput, not subject to electromagnetic interference, can cover great distances	Very expensive, requires physical wiring	N/A	N/A	N/A	$500	N/A
Uses existing cabling	Extremely slow, limited number of existing phone jacks	N/A	N/A	N/A	N/A	30 minutes
Uses existing cabling, backward compatible with HPNA 1.0 equipment	Extremely slow, limited number of existing phone jacks, hardware difficult to find	N/A	N/A	N/A	N/A	30 minutes
Fast enough for Internet and limited file sharing, uses existing cabling, backward compatible with HPNA 1.0 and 1.1 equipment; QoS (Quality of Service)	Not ideal for streaming video or audio, limited number of existing phone jacks, hardware difficult to find	$13	N/A	N/A	$13	30 minutes
Fast, uses existing cabling; QoS; backward compatible with HPNA 1.0, 1.1, and 2.0 equipment	Limited number of existing phone jacks, hardware difficult to find	N/A	N/A	N/A	N/A	30 minutes
Capable of carrying IPTV (Internet Protocol Television), HD audio, and video; uses existing cabling; QoS; backward compatible with HPNA 1.0, 1.1, 2.0, and 3.0 equipment	Limited number of existing phone jacks, standard not yet finalized	N/A	N/A	N/A	N/A	30 minutes
Fast enough for Internet and limited file sharing, uses existing cabling, uses readily available power outlets	Not ideal for high-bandwidth applications such as streaming video and audio	$25	N/A	$3 (USB cable)	$28	45 minutes
Uses existing cabling; uses readily available power outlets; capable of carrying IPTV, HD audio, and video; backward compatible with HomePlug 1.0; QoS	Equipment somewhat expensive	$130	N/A	$3 (USB cable)	$131	45 minutes
Fast enough for Internet and limited file sharing, inexpensive, good signal range, wireless	Slow, commonly suffers from interference	$25	$50	N/A	$42	1 hour
Fast enough for most applications, less interference with household electronics, wireless	Not natively compatible with 802.11b/g equipment	$30	$100	N/A	$64	1 hour
Fast enough for most applications, good signal range, backward compatible with 802.11b equipment, wireless	Commonly suffers from interference	$30	$50	N/A	$47	1 hour
MIMO (multiple-input multiple-output) technology, wireless	Standard not yet finalized	N/A	N/A	N/A	N/A	N/A

*network interface card

Network On The Cheap

How To Easily Network Two Computers

Can't we all just get along? If you have two computers and you want to share files and peripherals (such as a printer) between them, then the answer is a definite yes. And you can do it all for less than you might think.

The two-PC-file-sharing network is such a common network type that there are multiple ways of achieving this setup. This article will focus on how to network two computers using a 10/100 Ethernet crossover cable. Other types of direct-cable connection networks not covered in this article include Parallel interlink, serial null modem, USB, and FireWire.

The hardware required for this network is rather minimal. You'll need a single length of Ethernet crossover cable long enough to span the two computers, and both computers need to have an installed NIC (network interface card). Fortunately, most computers manufactured in the past decade come with 10/100 Ethernet NICs preinstalled.

Ethernet patch cables have identically wired plugs.

Keep Your Wires Crossed

Ethernet cables are commonly referred to as being either patch cables or crossover cables. An Ethernet patch cable, or straight-through cable, is what you typically use to connect your computer to a router, cable modem, hub, or switch. The two ends of an Ethernet patch cable look identical, with the colored wires appearing in the same order on each plug. An Ethernet crossover cable, sometimes called a reversed-wire network cable, features two of the four data wires (usually in a solid color) reversed. This essentially connects the data-transmitting pipe of one computer to the data-receiving pipe of the second computer and vice versa. If you used an Ethernet patch cable to connect two PCs, the data would fail to pass between the computers whenever both computers tried to send data at the same time. Crossover cables do not suffer from these collision problems, and are therefore ideal for direct-networking applications. At Newegg.com (www.newegg.com), we found a 7-foot length of crossover cable from Belkin for $2.99, but you can expect to pay as much as $20 or $30 if you purchase your cable at a

major retail outlet, such as Best Buy or Circuit City.

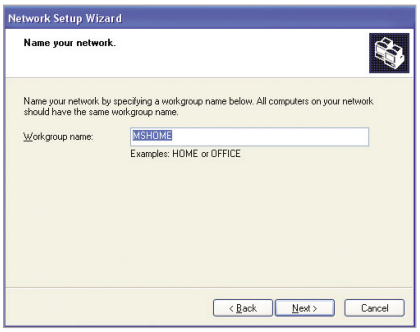
Hook 'Em Up

For our two-PC-file-and-printer-sharing network, we used two computers with Windows XP Home and preinstalled NICs. The procedures listed below also work for notebooks.

First, connect each end of the Ethernet crossover cable to the respective RJ-45 Ethernet ports of each computer's NIC. These ports look like large phone jacks. On a side note, if one of the computers you are using is connected to the Internet via wired Ethernet, and you only have one NIC installed in that computer, you may have to remove the Ethernet patch cable that connects your PC to your modem. For information on how to set up an Internet connection-sharing network, see "Share The Bandwidth" on page 65.

On each computer, click Start, click Control Panel, click Network and Internet Connections, and then click Network Connections. Right-click the Local Area Connection from the right pane of the window, and then click Properties. On the General tab, make sure there is a check in front of File and Printer Sharing for Microsoft Networks.

Back in the Network Connections folder, click Set Up A Home Or Small Office Network from the left side of the window. Click Next, and then


Network Setup Wizard
Name your network.
Name your network by specifying a workgroup name below. All computers on your network should have the same workgroup name.
Workgroup name:
MSHOME
Examples: HOME or OFFICE
< Back
Next >
Cancel

In the Network Setup Wizard, make sure the workgroup for both computers is the same.

Next again. Click the radio button in front of Other, click Next, click the radio button in front of This Computer Belongs To A Network That Does Not Have An Internet Connection, and then click Next. The Network Setup Wizard then asks you for a computer description and a computer name. Click Next after entering a name and description. On the following page you'll need to choose a workgroup name. By default WinXP names your workgroup MSHOME. Click Next, click the radio button in front of Turn On File And Printer Sharing (you won't see this screen if File And Printer Sharing is already enabled), click Next, and then click Next again.

After a short wait, the Network Setup Wizard gives you the option of creating a Network Setup Disk. Choose this option, and then click Next (make sure you have a blank floppy disc in the floppy drive). If both PCs use WinXP and you don't want to create a Network Setup Disk, you can simply launch the Network Setup Wizard on the second PC and configure it manually. Click Next to continue. Click Next and then click Finish to close the wizard. The computer will restart to enable the new network settings.

On the second PC, insert the Network Setup Disk into the floppy drive (or transfer the netsetup.exe file onto the other computer via USB thumb drive). Access the file and double-click it to start the Network Setup Wizard. Click Yes, click Next, and then click Next again. Follow the procedure listed above, making sure to name this second PC something different, but keeping the workgroup the same. Turn on File And Printer Sharing, click Next, and then click Next again. Select the option to finish the wizard now, click Next, and then click Finish. Your PC will need to restart to finalize the process.

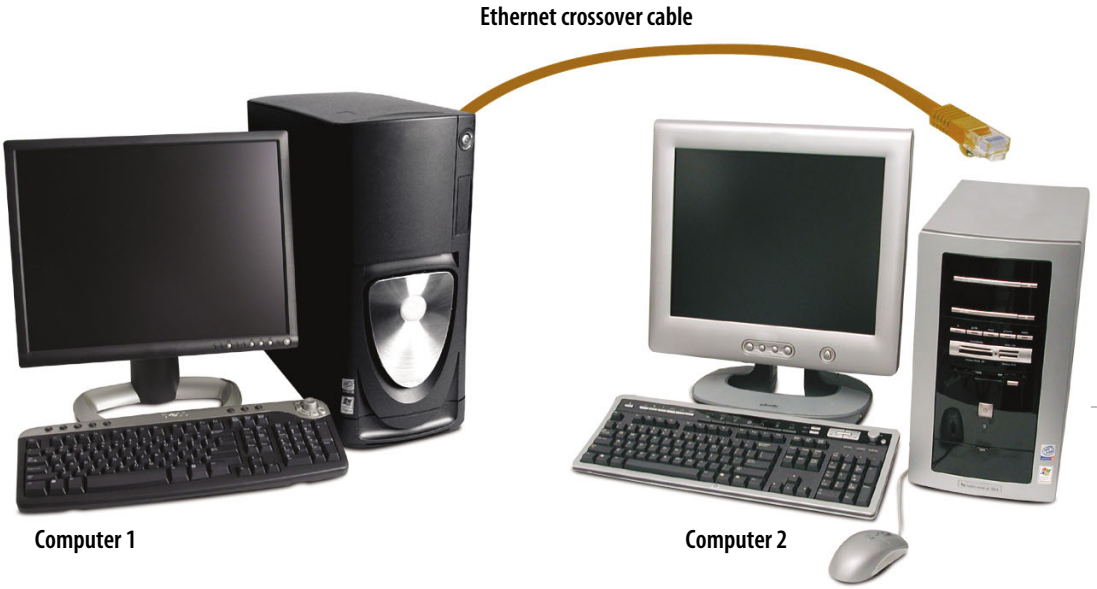
To see your networked computer, click Start, click My Network Places, and then click View Workgroup Computers from the list of Network Tasks on the left side of the page. You can share various folders by right-clicking them and clicking Sharing And Security. On the Sharing tab, click the check box beside Share This Folder On The Network. You can also let network users edit the files on this computer by checking the box directly below the folder's Share Name.

How To Configure Windows 98 On This Network

If one or more of the computers in your network uses Windows 98, you'll need to follow a slightly different procedure to create a network. Make sure you have your Network Setup Disk handy.

Insert the Network Setup Disk you created into the floppy drive of your Win98 computer. Double-click the netsetup.exe file to start the Network Setup Wizard. Click Yes, click OK, and then click Yes to restart your computer. Upon restart, the Network Setup Wizard will launch. Click Next, click Next again, click the radio button in front of This Computer Belongs To A Network That Does Not Have An Internet Connection, and then click Next. Give your Win98 PC a unique description and name, click Next, make the PC's workgroup the same as the other computers in your wired network, click Next, click Next again, and then click Finish. Restart your Win98 computer. To access the other computers connected to your network from the Win98 computer, just double-click the Network Neighborhood icon from your Desktop.

To share a folder, simply right-click the folder you want to share, click Sharing, click the Sharing tab, and then click the radio button in front of Shared As. Here you can change the Shared Name, and allow Read-Only or Full access rights. You can also set up a password from this dialog box. Click Apply and then click OK to close the dialog box.



As far as the hardware is concerned, creating a two-PC file-sharing network is a straightforward task.

Click Apply, and then click OK to close the dialog box.

Printer Sharing

To share the printer, make sure it's connected to a PC on your network. We recommend using the PC with the most up-to-date operating system. On that PC, click Start, click Settings, click Control Panel, and then double-click Printers And Faxes. Next right-click the printer you'd like to share and click Sharing. Click the Sharing tab, click the radio button in front of Share This Printer, and click OK. Your printer should now be shared.

At the second computer click Start, Control Panel, and then double-click Printers (in Win98/2000) or Printers And Faxes (WinXP). If you're viewing the Control Panel in Category View, click Printers And Other Hardware, and then click Printers And Faxes. Double-click Add A Printer to launch the Add Printer Wizard and then click Next. Click the Network Printer radio button and click Next. Click Next again to browse for a printer. In the Shared Printers box, double-click Microsoft Windows Network, then double-click the name of your workgroup (such as MSHOME), double-click the name of the computer to which the printer is physically connected, and then select the appropriate printer. Click Next and then click Next again to make this the default printer for this computer. Click Finish to close the wizard.

As you can see, building a two-PC-file-sharing network is one of the fastest and simplest ways to get your computers talking. Now you can retire the old download-it-to-a-floppy-and-huff-it-to-the-other-computer method of file sharing. Your feet will thank you. RS

BY ANDREW LEIBMAN

How To Configure Windows 2000 On This Network

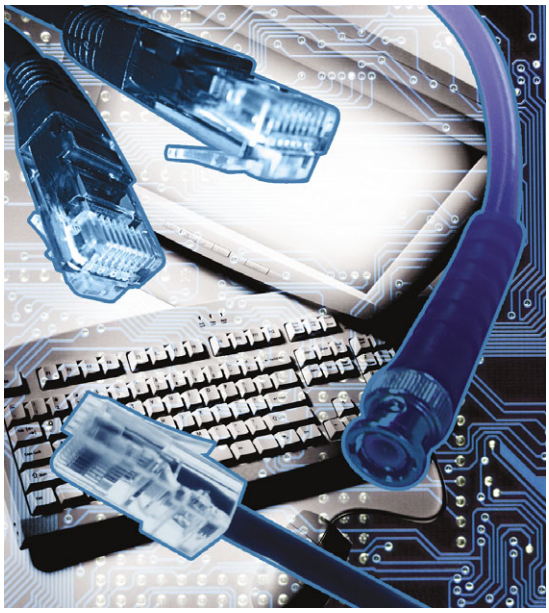
Windows 2000 doesn't include the Network Setup Wizard, so you'll need to follow a different procedure to add a Win2000 system to your network. On the Win2000 computer, click Start, Settings, Control Panel, and then double-click Network And Dialup Connections. Click the Network Identification link on the left side of this window, and then click Properties from the Network Identification tab. In the Member Of section of this dialog box, click the Workgroup radio button and type the name of your network's workgroup, for instance MSHOME. Click OK, click Apply, click OK to close the dialog box, and then click Yes to restart your computer.

The first time you try to access files on the Win2000 computer from another computer, you may need to enter the administrator's username and password. Use the username and password that you use to log on to the administrator account of the Win2000 machine. If you don't have a username and password in place on that computer, simply enter "administrator" for the username, leave the password field blank, and then click OK.

To share a folder on your Win2000 machine, simply right-click the folder you want to share, click Sharing, click the Sharing tab, and then click the radio button in front of Share This Folder. Here you can change the Share Name and the permissions settings. Click Apply and then click OK to close the dialog box.

Getting Wired & Going Wild

How To Set Up A Wired Network



If you use multiple computers on a regular basis in your home or business, networking them just makes sense. Building a wired network is a cheap and easy way to access anything from any computer. For instance, you might have one computer that offers more storage capacity, a second computer with superior hardware, and a third all-purpose computer connected to the Internet and a printer. Wire them all together and you've essentially created one computer that lets you access everything you need.

The previous article showed you how to create a wired LAN (local-area network) between two computers using an Ethernet crossover cable. If you're interested in networking three or more computers, however, you'll need a slightly different setup. Before you set out to make your own network, you'll need the right hardware and a few other odds and ends in place first.

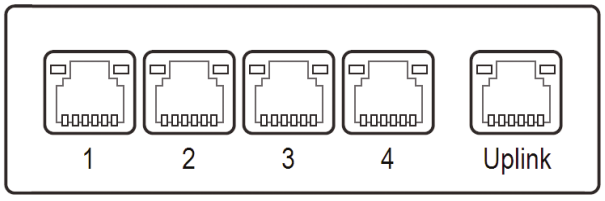
Network adapters. Each computer must include a network adapter, either integrated into the motherboard or in the form of an expansion card, also called a NIC (network interface card). You can verify whether or not your computers have network adapters by looking for an RJ-45 Ethernet port on the back of each system you'd like to network. If one of your computers doesn't have an Ethernet port and you have an available expansion slot in your computer, you can purchase a network adapter for about $20.

Hubs, switches, and routers. As discussed in the previous article, an Ethernet crossover cable connects the data transmitting pipes of one computer to the data receiving pipes of the second computer. Things get a bit more complicated when you add a third computer to the mix. A hub, switch, or router is necessary to juggle the data traffic constantly coming and going between the networked computers and peripherals. Each device lets you network your computers, but there are differences.

The hub is the most simplified of the three devices and typically features two or more Ethernet ports for connecting networkable devices. A switch is essentially a piece of hardware (sometimes embedded in a router or hub) that filters and quickly forwards data from its source to its intended destination. Switches are more useful in large networks where data traffic gets too cumbersome for a simple hub or router. A router works similarly to a switch, but its aim is to receive data from networked devices or computers and forward it to the intended destination using the shortest route possible. The router takes into account various factors when choosing the shortest route, including Internet traffic, throughput capacity, and other conditions. As a result, routers tend to hand off data more slowly than switches. For most home users, a hub is more than sufficient for networking three or more computers.

Ethernet cable. The final component to our network is the physical wiring you'll use to connect the computers to the hub. For this network, you'll need a length of Ethernet patch cable, also called straight-thru cable, for each computer you want to network. Crossover cables aren't necessary for this type of network. To distinguish a crossover cable from a straight-thru cable, compare the two plugs of each cable. A straight-thru cable will feature plugs with the colored wires in the same order from left to right while a crossover cable features plugs with one pair of colored wires reversed.

You'll notice that there are multiple cable types, or categories, that you can use. The older specification, called Category 5, or CAT5 for short, has a throughput capacity of up to 100Mbps (megabits per second). Category 5e, or



A typical hub features multiple RJ-45 ports for networking computers.

CAT5e, cable features better insulation and can handle throughputs up to 1000Mbps. Category 6, or CAT6, cable supports the same speeds as CAT5e, but only works with CAT6-certified equipment. CAT6 cable is even less susceptible to unwanted interference.

We recommend using CAT5e cable for your wired network because it supports a wide spectrum of throughput speeds and is relatively common.

Speed-Conscious

If you're assembling a network from scratch, consider purchasing networking equipment that can handle the fastest throughput commonly available. Gigabit Ethernet can support transmissions at up to 1000Mbps, which is ideal for streaming media such as high-definition video. Even if you don't plan on streaming high-definition video right now, Gigabit Ethernet is the most future-proof option if you decide to stream hi-def video later, and Gigabit-capable hardware is only marginally more expensive. 10/100 Ethernet, also called Fast Ethernet, is usually a cheaper option capable of supporting 100Mbps speeds, which is more than sufficient for sharing an Internet connection and transferring decent-sized files between your networked computers.

If your computers already have network adapters (most newer systems do), you can check the speeds they support by right-clicking My Computer, clicking Manage, clicking Device Manager from the left pane of the Computer Management window, and then clicking the plus (+) in front of Network Adapters. Make sure your hub and network adapters all support the same speeds; if even one component is slower than the rest, the whole network will only operate at the speed of that slower component. For more information

Upgrade Your Wired Network

You can get more out of your network by upgrading your network speed or adding another node (such as a computer, server, or printer). For more information about wireless networks, see "Wires: Who Needs 'Em?" on page 32.

Accelerate your network. The procedure for upgrading your network speed is roughly the same whether you're upgrading your 10/100 Ethernet network to handle high-definition media files, or you're clawing your way out of the 10Mbps (megabits per second) Stone Age.

Before you upgrade the speed of your wired network, you have to know your network's current capabilities. On each of your networked computers, right-click My Computer, click Manage, click Device Manager, and then click the plus (+) in front of Network Adapters. You should see the manufacturer and model of your network adapter, as well as its speed. As stated above, your network will only operate at the peak theoretical speed of your slowest component, so you may not need to buy all new hardware. For instance, if your current network consists of a 10/100 hub, two 10/100 computers, and an older computer with a 10Mbps network adapter, then you can experience a big leap in performance by simply installing a 10/100 network adapter into your older computer.

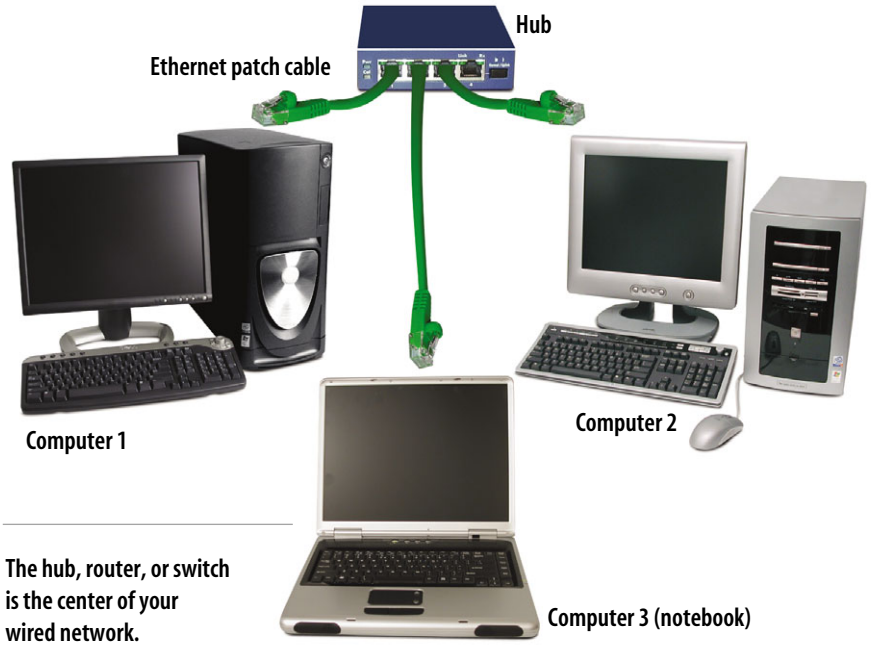
If, on the other hand, all components of your network operate at 10Mbps, or at a faster-but-not-fast-enough 100Mbps, you'll probably need to buy a new NIC (network interface card) for each PC; a new hub, router, or switch; and possibly new Ethernet cables. Remember, CAT5 cable works at 100Mbps, and CAT5e and CAT6 cable work at Gigabit speeds.

Start by disconnecting the Ethernet cables running between your computers and the hub. Carefully follow the instructions for installing the new NICs in each of your network computers and then make sure each is enabled and working in the Device Manager. Turn all systems off again and then connect the Ethernet cables to the new hub. Boot your computers one at a time, configuring them as described in the main section of the article, if necessary.

Add a node. The method of adding another component to your wired network depends heavily on the current hardware you're using in your network. If you're using a crossover cable to connect two computers and a printer and you'd like to add another computer, then you'll need a hub, router, or switch as your central connecting device and some Ethernet patch cable to span between it and each of your computers.

If you already have a hub, router, or switch, then you'll need a free port on the back of the unit for each computer you'd like to network. If your hub doesn't have any free ports available, then you'll need to purchase a new one. As we went to press, we found 4-port hubs for less than $25 and 8-port hubs for less than $50 and both supported networking speeds of up to 100Mbps. The computer you're adding to the network also needs a NIC or an integrated network adapter, preferably capable of the same speeds as the rest of the networking hardware you're using. Turn the new computer off, plug one end of a length of Ethernet patch cable into the RJ-45 port on the back of the computer, and then plug the other end into the free port on the hub. Turn the computer on. Using the procedure detailed above, run the Network Setup Wizard on the new computer. Make sure to give your new computer a unique name, but the same workgroup name as the rest of the computers on the network.

If you're adding a printer, you can purchase a hub, router, or switch that features a standalone printer port, or simply connect the printer to one of the currently networked computers and enable printer sharing. For more information on networking with printers see "Print Connections" on page 62.



The hub, router, or switch is the center of your wired network.

on how to upgrade the speed of your wired network or add a wired node, see the Upgrade Your Wired Network sidebar on the previous page.

Make Contact

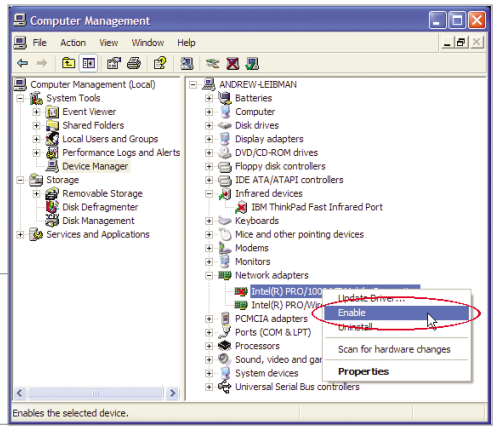
The following instructions also work if one of the computers in your potential network is a notebook. Throughout the article, we'll refer to the centerpiece of our network as a hub, even though a router or switch will work the same way.

Before you assemble the network, make sure that the network adapter in each computer is enabled. To check the network adapter's status, click Start, click Control Panel, click Network And Internet Connections (if you're viewing the Control Panel in Category View), and then click Network Connections. If you're viewing the Control Panel in Classic View, simply double-click Network Connections. If your network adapter is enabled, you will see the Local Area Connection icon. You can skip the next two paragraphs if your network adapter is working.

Fix it from the Device Manager. You can enable your network adapter using the Device Manager and install its drivers (if necessary). Right-click My Computer, click Manage, click Device Manager from the left pane of the Computer Management window, and then click the plus (+) in front of Network Adapters. If you see a yellow question mark under Network Adapters, then you'll most likely need to install the driver. You can typically find your network adapter driver on a disc that came with the network adapter or PC. If you have neither, check the adapter manufacturer's Web site. After you install the drivers, right-click the adapter listed in the Device Manager list and then click Enable. You will need to make sure the network adapter for each computer is up and running before you can continue.

Fix it from the BIOS. If the Local Area Connection icon is missing, then your network adapter may be disabled. To enable an integrated network adapter, you may need to use the computer's BIOS (Basic Input Output System) menu. To do this, restart your computer and enter the BIOS setup utility by pressing DELETE, F1, or another function key during the first part of the boot process. Often, instructions for accessing the BIOS setup utility appear briefly on-screen as the computer boots. (You may need to consult your motherboard or PC manual for the proper key.) Navigate through the BIOS menu and enable the Onboard LAN, Onboard Network, or Onboard Ethernet. You'll commonly find these options in the Integrated Peripherals, Peripheral Configuration, or I/O Devices submenu (menu names vary by manufacturer). Save the BIOS settings and restart the computer (instructions for saving and restarting are usually at the bottom of the BIOS setup utility screen).

Plug it in. Before you begin connecting your network, shut down each computer and grab your network hub and network cables. The ports on the hub are typically numbered. Connect your main computer to the first port on your hub (usually labeled as such) and then connect the remaining computers to ports 2, 3, and so on. You may want to label each cable near the hub so you know which plug corresponds to which computer. Don't connect any of your computers to the Uplink, WAN (Wide-Area Network), Internet, or Broadband Modem port on the hub, if it has one. You use this port to connect your hub to the Internet through a cable or DSL



You can make sure your network adapters are enabled by checking the Device Manager.

(Digital Subscriber Line) modem. For more information on configuring ICS (internet connection sharing), see "Share The Bandwidth" on page 65.

Next plug the AC adapter for the hub into an electrical outlet, turn it on, and then power on the computers in your wired network. On the main computer, click Start, click My Computer, and then click the My Network Places link from the left side of the window. You may not see the other computers in your network immediately, but give it a couple minutes to scan for the connected computers. If the computers don't appear, you may need to manually configure your network.

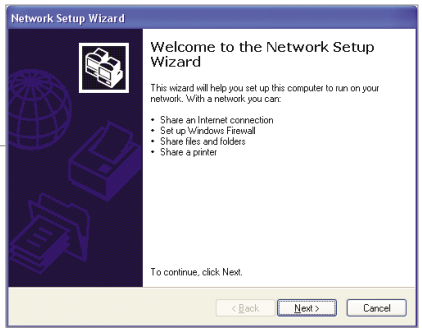
Network Setup Wizard

To manually configure your computer's connection, click Start, click Control Panel, click Network and Internet Connections, and then click Network Connections. If you're viewing the Control Panel in Classic View, just double-click Network Connections. Click the Set Up A Home Or Small Office Network link from the left side of the window.

The Network Setup Wizard can help you share an Internet connection, configure the Windows Firewall, share files, and share a printer.

Click Next to continue from the Network Setup Wizard's welcome screen. This page features a Checklist For Creating A Network link. We've already completed the steps detailed on this screen, so click Next to proceed. If the following screen says that the wizard found disconnected network hardware, click the checkbox in front of Ignore Disconnected Network Hardware, and then click Next.

The Network Setup Wizard then asks you to choose the statement that best describes your computer. The top two options concern how your computer connects to the Internet (either directly or through another computer). You can click the links to view examples or click the Home Or Small Office Network Configurations link to open the Help And Support Center. For the purposes of this article, click the radio button in front of Other, click Next, click the radio button in front of This Computer Belongs To A Network That Does Not Have An Internet Connection, and then click Next.


Network Setup Wizard
Welcome to the Network Setup Wizard
This wizard will help you set up this computer to run on your network. With a network you can:
• Share an Internet connection
• Set up Windows Firewall
• Share files and folders
• Share a printer
To continue, click Next.
< Back
Next >
Cancel

On the following page, enter a computer description and a computer name. According to the Help And Support Center, the computer name identifies your computer on the network. No two computers on your network can have the same name, so choose something unique. Your computer's name can be up to fifteen characters long with no spaces or special characters. If you're only networking a handful of computers you can rely on the computer's location for your computer's name, such as "office" or "den."

If you're connected to the Internet, your ISP (Internet service provider) may have assigned your computer a specific name that identifies it on the ISP's network. Check with your ISP to see if this is the case. If it is, don't alter the computer name.

You have a little more freedom with the computer description. Here you can provide a brief explanation of the computer. If the computer is used primarily by a single person, then, for instance, you can describe the computer as Paige's Computer. Only Windows XP computers display a computer description. Click Next to continue.

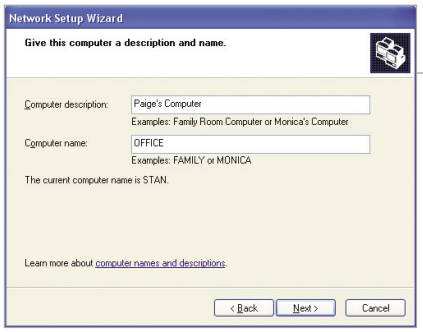
This page asks you to specify a workgroup name. Every computer on your network must have the same workgroup name. By default, Windows suggests the workgroup name MSHOME. Click Next, click the radio button in front of Turn On File And Printer Sharing, and then click Next.

How To Configure Windows 98 On This Network

Thanks to the Network Setup Wizard, the process of configuring a Windows 98 PC is similar to the process involved in configuring a Windows XP PC.

Insert the Network Setup Disk into the floppy drive (or transfer the netsetup.exe file onto the second computer via floppy disk). Navigate to and double-click netsetup.exe to start the Network Setup Wizard. Click Yes, click OK, and then click Yes to restart your computer. If you used a floppy disk, make sure you remove it before the computer restarts. Upon restart, the Network Setup Wizard will launch. Click Next, click Next again, click the radio button in front of This Computer Belongs To A Network That Does Not Have An Internet Connection, and then click Next. Give your Win98 computer a unique description and name, click Next, make the computer's workgroup the same as the other computers in your wired network, click Next, click Next again, and then click Finish. Restart your Win98 computer to enable the settings. To access the other computers connected to your network from the Win98 computer, just double-click the Network Neighborhood icon from your Desktop.

To share a folder on a Win98 computer, simply navigate to the folder you want to share, right-click it, click Sharing, click the Sharing tab, and then click the radio button in front of Shared As. Here you can change the Shared Name and modify the access rights. You can also set up a password from this dialog box. Click Apply and then click OK to close the dialog box. ▌



The computer name and description for each networked computer should be unique.

The screen now displays a quick summary of the settings you're applying to your network computer. Double-check the settings and click Next. The process of configuring your computer may take a minute or so.

The next page of the Network Setup Wizard lets you create a Network Setup Disk. This step isn't necessary if all the PCs on your network have WinXP. Insert a blank floppy disk or a removable flash drive, click the radio button in front of Create A Network Setup Disk, and then click Next. Choose the media upon which you want to copy the Network Setup data and click Next to continue. Click Next again to display a list of instructions for configuring the other computers on your network. Click Finish and then click Yes to restart your computer.

Set up your other computers. To set up your non-WinXP network PCs, insert the Network Setup Disk into the floppy drive (or transfer the netsetup .exe file onto the second computer via a removable flash drive). Navigate to and double-click netsetup.exe to start the Network Setup Wizard. The Network Setup Wizard will start by installing support files on this computer. Click Yes to continue. If your other computers have WinXP, then simply run the Network Setup Wizard as described above. Click Next, and then click Next again. Click the radio button in front of Other, click Next, select the radio button in front of This Computer Belongs To A Network That Does Not Have An Internet Connection, and then click Next.

If your second computer has more than one network adapter, you may get the option to let the Network Setup Wizard determine the appropriate connection automatically, or choose the connection yourself. If you encounter this screen, choose the former option and click Next. Choose a unique name and description for this second computer (unless the computer name was assigned by your ISP) and click Next. On the next page, make sure the workgroup is the same as that of the initial computer, such as MSHOME, and then click Next. Review the Network Settings on this screen, click Next, click the radio button to Just Finish The Wizard, click Next, and then click Finish. Click Yes to reboot your computer. Repeat this process for all of your networked computers.

View your network. Now that your network is set up, let's check it out. Click Start, click My Computer, and then click the My Network Places link on the left side of the page. Click View Workgroup Computers from the list of Network Tasks on the left side of the page. You should see the other PCs connected to your network.

If you want to share a folder, open My Computer and navigate to the folder, then right-click the folder and click Sharing And Security. On the Sharing tab, click the check box beside Share This Folder On The Network, click Apply, and then click OK to close the dialog box.

You don't need to max out your credit cards and sell your organs to afford your own super computer. With a wired network, you can distill your separate computing resources into a single unit capable of offering the best of each system. And that lets you get more done, no matter which computer you're using. RS

BY ANDREW LEIBMAN

How To Configure Windows 2000 On This Network

You'll need to manually configure the network settings on a Windows 2000 computer because this operating system doesn't include the Network Setup Wizard. Click Start, Settings, Control Panel, and then double-click Network And Dialup Connections. Click the Network Identification link on the left side of this window, and then click Properties from the Network Identification tab. Click the Workgroup radio button in the Member Of section of this dialog box, type the name of your network's workgroup, for instance MSHOME, and then click OK. You should see a pop-up message welcoming you to the workgroup. Click OK to close the pop-up, click OK to close the Identification Changes dialog box, click OK again to close the System Properties dialog box, and then click Yes to restart your computer.

When accessing files from the Win2000 computer over the network, you'll have to input the administrator's username and password. Use the username and password that you use to log onto the administrator account of the Win2000 machine. If you don't have a username and password in place on that computer, simply enter "administrator" for the username, leave the password field blank, and then click OK. You should only have to enter the username and password the first time you make a connection. To access other computers from your Win2000 computer, access My Computer, click the My Network Places link from the left side of the page, and then double-click Computers Near Me.

If you want to share individual folders on your Win2000 computer, right-click the folder, click Sharing, click the Sharing tab, and then click the radio button in front of Share This Folder. This dialog box lets you change the folder's Share Name and change the permissions settings. Click Apply and then click OK to close the dialog box. ❙

Wires: Who Needs 'Em?

How To Install A Wireless Network

Going wireless is one of the most hassle-free ways to go whether you're setting up your first network, or just looking to break the chains of your current wired network. According to D-Link's Technical Media Manager, Mike Scott, "I don't know anybody who'd have an Ethernet port out by their pool." In addition to the ability to roam freely, wireless networks also let you expand or shrink the number of computers or other networked devices on the fly, without having to poke holes in your walls or run cable through hallways and above doorways. Even no-new-wires options, powerline systems, still require a length of Ethernet, USB, or phone cable running from a wall outlet or phone jack to complete the connection, which only adds to the clutter of cables stuffed behind your computer tower.

Another argument for wireless networks is the ease with which you can network mobile devices such as Wi-Fi-capable notebooks and PDAs. And making your wireless network secure is straightforward and easy to do. As the price of wireless networking hardware continues to fall, now is a great time to consider cutting those wires. For our wireless network, we'll be connecting three computers together using 802.11g networking equipment. We'll go into more detail about the wireless networking standards below, but first let's start with what you need to get your wireless network up and running.

Wireless Checklist

The hardware involved in setting up a wireless network is similar to that which is necessary for a wired network. Each computer in your network will need a wireless network adapter to send and receive wireless signals. You'll need a central networking device, such as an access point, gateway, or router, that juggles the data going to and from each networked computer.

Wireless network adapters. If your computer has a free PCI (Peripheral Component Interconnect) slot, you can purchase and install an internal wireless network adapter. If you don't have a free slot, or just feel uncomfortable opening your computer case, you can purchase an external wireless network adapter and connect it to a free USB port on the PC.

Because they are valued for their mobility, most notebooks available today feature integrated wireless network adapters. To determine if your notebook has an integrated wireless network adapter, click Start, right-click My Computer, click Manage, click Device Manager in the left pane, and then click the plus sign in front of Network Adapters. If one of the items listed under your Network Adapters is wireless, then you're all set. You can connect older notebooks to your wireless network using a PC Card-based wireless network adapter. Desktops, on the other hand, aren't typically built to roam around your home or business, and therefore usually come with some form of wired network adapter. A quick way to determine if your desktop has a wired or wireless network adapter is to check the back panel of the tower. If you see a thick plastic antenna, then you have a wireless network adapter already installed. For the vast majority of desktops, however, you'll probably find one or more RJ-45 ports, which look like large phone jacks. These connect to the network adapters that your desktop uses to communicate with other computers in a wired network.

You can install wireless network adapters in each computer and set them up in what most configuration applications call **Ad-Hoc Mode** (or as a peer-to-peer network). Ad-Hoc Mode simply refers to a network that consists of computers that communicate one-on-one via wireless network adapters alone (that is, without an access point or base station, which is a device that manages the flow of data to and from all of your networked computers). This article will focus on building a network using Infrastructure Mode (also known as hosted or managed mode), which requires a wireless adapter in each computer and a centrally-located access point. This configuration lets you more easily share a cable or DSL (Digital Subscriber Line) Internet connection and add both wired and wireless nodes as your network expands.

USB network adapters are an easy way to add wireless capabilities to an older computer.

Access points, gateways, and routers. Typically an access point features multiple LAN (local-area network) ports for connecting wired nodes, a single WAN (wide-area network) port for connecting a cable or DSL modem, and at least one antenna for broadcasting and receiving wireless signals. A wireless router or gateway is essentially an access point that adds firewall, filtering, and switching functions. Although these functions aren't necessary to set up a wireless network, they can improve your network's security.

802.11 Who?

When building a wireless network, you'll need to make sense of the different wireless languages, or standards, that computers use to communicate with each other. As a standards-making body, the IEEE (Institute of Electrical and Electronics Engineers) has established a handful of wireless networking protocols that you'll need to be aware of when shopping for parts. Some standards are interoperable and others aren't, but whichever standard you choose, it's best to use a single standard to get the best performance for your dollar.

802.11b. The initial Wi-Fi standard, 802.11b, debuted in 1999. The standard operates within the 2.4GHz radio band (frequencies between 2.4GHz and 2.483GHz) to deliver a theoretical maximum data throughput of up to 11Mbps (megabits per second) at distances of up to 300 feet (in ideal circumstances). The 802.11b wireless standard is currently a popular choice because it is inexpensive and widely available (and therefore widely compatible). An 802.11b wireless network can handle a broadband Internet connection, file transfers, and gaming.

If you install an 802.11b wireless network, you can expect real-world connection speeds of about 6.5Mbps. If a given computer's network adapter is more than 100 feet from an access point or base station, you can expect that number to drop to 4Mbps or lower. Speed-wise, 802.11b currently occupies the low-end of the networking spectrum. If you're looking to stream high-definition video and audio content between your networked computers, then 802.11b isn't going to cut it. Another drawback of 802.11b includes its tendency to experience interference with other electronic devices that work within the 2.4GHz radio band, such as microwaves, Bluetooth devices, and cordless phones.

802.11a. Although the IEEE ratified the 802.11a standard at roughly the same time as the 802.11b standard, it has not seen as much popularity in the consumer market. 802.11a operates at the 5GHz radio band and supports data rates of up to 54Mbps. The 802.11a signal is effective at up to 150 feet indoors, but you can expect throughputs to hover between 20 and 25Mbps under typical conditions. 802.11a's 5GHz operating frequency isn't shared with other electronic devices, which means that it is much less prone to interference. The faster data rates also make 802.11a networking equipment an attractive buy, but the signal degrades much more quickly than 802.11b equipment. This means that to cover the same area as an 802.11b network and maintain the superior connection speed, you'll typically need more 802.11a access points.

802.11g. In 2003, the IEEE cobbled together a best-of-both-worlds standard in the form of 802.11g. This standard utilizes the same 2.4GHz radio band as the 802.11b standard, but can achieve data rates of up to 54Mbps (or 20 to 25Mbps under typical conditions). Because 802.11g uses the 2.4GHz radio band, it too is susceptible to interference from other electronic devices. And although 802.11g equipment is interoperable with 802.11b equipment, a network consisting of mixed hardware will only operate at the peak speed of the slowest piece of hardware. 802.11g equipment is popular in both consumer and enterprise markets, is widely available, and is becoming increasingly inexpensive.

Not long after 802.11g's debut, chip manufacturers began to stretch the standard's upper speed capabilities based on aspects of a then-unreleased version of the 802.11e standard. Various wireless hardware manufacturers began offering enhanced 802.11a and 802.11g hardware, with features named 802.11g+, Turbo Mode, Super G, and Xpress, which increase data rates using some form of data compression, **packet bursting** (decreasing the overhead of wireless communications), **fast frames** (increasing the number of bits sent at once and accelerating the timings of each transmission), and combining of multiple channels. The packaging for these devices often claims data rates up to 108Mbps, but real-world tests reveal that the upper-limit is closer to 90Mbps. The drawback of these technologies is that one manufacturer's speed-boosting scheme may not work with that of another manufacturer.

Jack of all modes. When shopping for wireless equipment, you're likely to encounter terms such as dual-mode, multimode, and tri-mode. Dual-mode or multimode equipment typically refers to adapters and access

points that support the 802.11b/g standard. Tri-mode equipment operates at both the 2.4GHz and 5GHz radio bands, making it compatible with any 802.11a, b, or g wireless network. It's for this reason that most business-class notebooks currently ship with tri-mode wireless network adapters. Tri-mode equipment is typically more expensive and generally unnecessary for most users.

What's next. Although 802.11a-, b-, and g-standard equipment is currently popular and readily available, the next phase of wireless technology is just on the horizon. The 802.11n standard is currently undergoing the final stages ratification, and promises to deliver data throughputs of up to 540Mbps. Early revisions of the standard also offer better ranges than those of currently available standards. Some manufacturers have already begun offering "draft" 802.11n equipment, but because the standard isn't finalized, the access points and network adapters from one manufacturer may not work with those from another. As we went to press, the final revision of the 802.11n standard is estimated for approval in mid-2007.

Hardware Where

Before you start to install and configure your wireless equipment, it's important to carefully consider the placement of your wireless access point within your home or business. Although the wireless protocols described above have ranges of between 150 and 300 feet, those distances are only effective under the most ideal conditions. You'll get the best connection speeds closest to the access point. Your wireless network can experience performance degradation if the wireless signal needs to pass through walls, heating and air-conditioning ducts, large metal objects, or floors. Positioning your wireless equipment near electronic devices such as microwaves, or other wireless-capable devices such as cordless phones or Bluetooth equipment, can also negatively affect your wireless network performance.

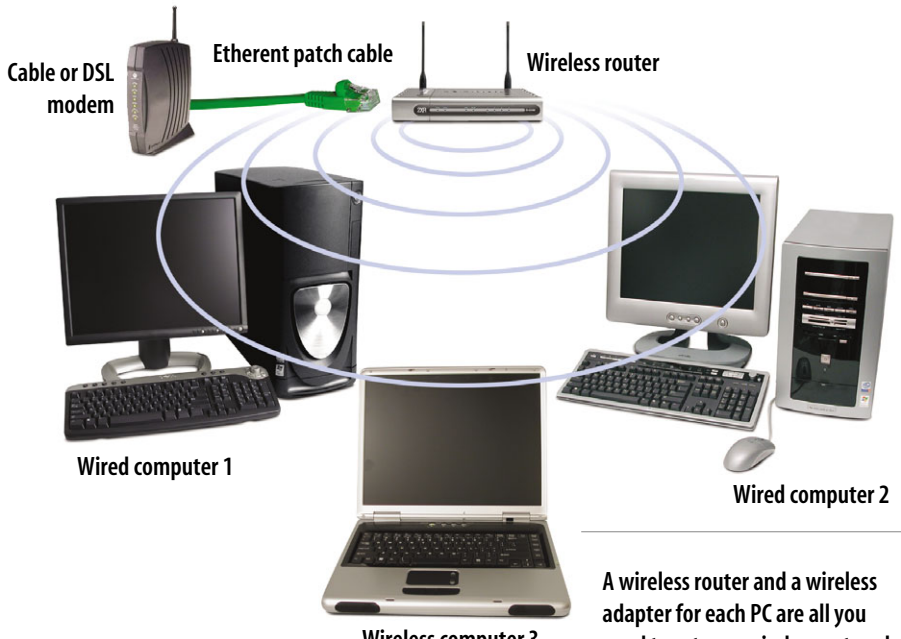
Make sure to take into account the current location of your cable outlet or phone jacks if you plan to connect a cable or DSL modem to your access point. If you want to save yourself some cash, you can use an Ethernet cable between the wired network adapter in your main computer and one of the Ethernet ports on your access point. This requires that you keep your access point fairly close to your main computer, but also saves you the cost of another wireless network adapter.

Make Contact

The first step in setting up your wireless network is to install the wireless access point. Consult the instructions supplied with your hardware for the proper procedures. According to our D-Link (www.dlink.com) 802.11g router's instructions, start by connecting the power adapter to both the router and a power outlet. The next step is to unplug your DSL or cable modem, and then connect a length of Ethernet cable between the WAN port of the wireless access point or router and the RJ-45 port of the DSL or cable modem. Next connect a length of Ethernet cable between the first LAN port on the back of the wireless access point and the RJ-45 port on the back of your main computer. This connection is only temporary if you plan on installing a wireless network adapter in the computer you are using to configure the wireless access point.

The next task is to configure the access point. Typically, wireless access points, routers, and gateways require you to either install the included software or type a static IP (Internet Protocol) address into your Web browser to access a configuration page. The instructions for our D-Link router require the latter method. Type the static IP address (such as http://192.168.0.1) into the address field of your browser and then press ENTER. A logon popup will appear. Type **admin** into the User Name field, leave the Password field blank, and click OK.

The configuration wizard will walk you through the process of enabling a password, choosing a time zone, and setting up an Internet connection. On the D-Link configuration



A wireless router and a wireless adapter for each PC are all you need to set up a wireless network

wizard, click Next to advance beyond the Welcome Screen. The following screen asks for a new password. Type a password you can easily remember, but that is difficult for an unauthorized user to guess, and then verify that password by typing it again. Click Next to continue. Choose your time zone from the drop box and click Next.

The following screen lets you select an Internet connection type. Some configuration wizards can automatically detect your Internet connection type. If this is the case, you can skip this step. Depending on your ISP (Internet service provider) you will need to choose Dynamic IP Address, Static IP Address, or PPPoE (Point-to-Point Protocol over Ethernet). You may see other options, but these three types are the most common. If you're unsure which option to choose, check with your ISP. Click Next to Continue. If you chose Dynamic IP Address, you'll need to enter a host name or MAC (Media Access Control) address, or leave the fields untouched if they were already detected and marked as optional. If you chose Static IP Address, then enter the WAN IP Address, Subnet Mask, Gateway Address, and a Primary DNS (Domain Name System) Address as per your ISP's instructions. If you chose PPPoE, you can enter your username and password (if required by your ISP).

Next you'll need to choose an SSID (Service Set Identifier) and set a channel. It's important to choose a unique SSID as an added layer of security. Make sure you enable the highest-level of WEP (Wired Equivalent Privacy) or WPA (Wi-Fi Protected Access) encryption (if available), and write down your encryption key. When you're finished with the configuration wizard, restart your computer.

The next step is to install wireless network adapters into each of the computers you want to network. If you're using a PC Card or USB-based wireless network adapter, installation is as simple as plugging the device into the appropriate port on your computer. You'll want to closely follow the instructions included with your hardware, as the step order can vary by manufacturer and model.

Our D-Link 802.11g network adapter required that we install the adapter's drivers prior to physically installing the card. If your instructions are similar, you can follow along. Insert the driver disc into the PC you connected to the wireless access point and install the drivers using the installation wizard (the exact steps may vary). Once the drivers are installed, click the radio button in front of No, I Will Restart My Computer Later, and then click Finish to close the wizard. With the driver disc still in your CD-ROM drive, shut down the computer.

Next, unplug your computer's power cord and remove the cover or side panel to access the inside of the case. Before touching any of your computer components, touch a metal part of the interior of the case to dispel static electricity. You can also use an antistatic wristband for this purpose. Use a screwdriver to remove the metal backplane adjacent to the PCI slot you're planning on using. PCI slots

Upgrading Your Wireless Network

If you have an 802.11b wireless network, then you already know the joys of wireless. But if you're feeling a little behind the times with your 11Mbps (megabits per second) peak data rates, then upgrading your wireless network can be a simple way to bring your wireless network up to speed. For this upgrade, we'll be swapping our 802.11b access point and network adapters for 802.11g equipment. Remember, you'll need to upgrade all of your components to the same standard in order to fully enjoy the benefits of that standard.

Before starting, you'll want to make note of the WEP (Wired Equivalent Privacy) or WPA (Wi-Fi Protected Access) encryption key, SSID (Service Set Identifier), and channel setting for your current access point, router, or gateway. You can obtain the SSID and channel settings from your current access point's configuration menu (menu layout varies by manufacturer). If you enabled WEP or WPA encryption, then you'll need to remember those keys. If you've forgotten them, you can establish new keys when you configure your new access point. Next, unplug and disconnect both your old access point and your DSL (Digital Subscriber Line) or cable modem. Plug in the new access point and connect a length of Ethernet cable between the WAN (wide-area network) port of the new access point and the RJ-45 port of the DSL or cable modem. Next, connect a length of Ethernet cable between the first LAN (local-area network) port on the back of the wireless access point and the RJ-45 port on the back of your main computer.

Follow the instructions for installing your new access point. Typically this involves either installing software or typing a static IP (Internet Protocol) address into your Web browser to access a configuration page. Using the access point's configuration menus, input your old access point's SSID, WEP, or WPA encryption key, and channel. With the access point successfully configured, you can remove the Ethernet cable between your main computer and the access point.

Next, install your 802.11g network adapters by following the instructions that came with your hardware. With the network adapters successfully installed, click the Wireless Network Connection icon from the System Tray, and then click View Wireless Networks. Click your wireless network, and then click the Connect button. If applicable, enter the WEP or WPA key into the appropriate field. Press ENTER, and wait for your computer to connect.

are long and rectangular-shaped, usually white or off-white in color, and often labeled on the motherboard as such. Insert the wireless network adapter all the way into the slot. Screw the adapter's backplane to the case and, if necessary, install the antenna. Next close the computer case, plug the computer in, and then power it on.

The New Hardware Wizard should appear. Click the radio button in front of Install The Software Automatically, click Next, and then click Continue Anyway if you encounter any Windows Logo Testing pop-ups. Click Finish to close the wizard. If the New Hardware Wizard didn't launch automatically, you can verify that the device installed correctly by checking the notification area of the System Tray (lower-right corner). If you see an icon for your wireless adapter, then it installed properly. Repeat this process for each computer.

With your hardware in place, each computer with a wireless network adapter should be able to detect your wireless network. On each computer in the network, click the Wireless Network Connection icon from the System Tray. The available wireless networks should appear in the right pane of the Wireless Network Connection window. Click your wireless network and then click the Connect button in the bottom-right corner of the window. If you enabled WEP or WPA encryption, then enter the key into the appropriate field. Press ENTER, and wait for your computer to connect. With your primary computer connected to the access point, you can now remove the Ethernet cable you used to span between the computer and the wireless access point.

Share Files & Printers

To enable file sharing over your newly established network, right-click any folder or hard drive letter you want to share, click Sharing And Security, and then click the check box in front of Share This Folder On The Network. This dialog box also lets you change permission rights by clicking the Allow Network Users To Change My Files check box. Click OK to close the dialog box.

To share a printer, go to the computer to which the printer is connected, click Start, click Control Panel, and then double-click Printers And Faxes. Next, right-click the printer you'd like to share and click Sharing. Click the radio button in front of Share This Printer on the Sharing tab, and then click OK. On each of the other computers in your network, open up the Printer And Faxes window and click Add A Printer. Click Next, click the radio button in front of A Network Printer, Or A Printer Attached To Another Computer, click Next, and then click the radio button in front of Browse For A Printer. If your computer is connected to a print server, you can click the appropriate radio buttons on this page and enter the Name or URL (uniform resource locator). Click Next, and then navigate through the Shared Printers box to select the appropriate computer and then the shared printer.

For most, building a wireless network is an exercise in practicality. Living wire-free means no tangled mess, no maintenance, and no new holes in your walls. But the real benefits of wireless become evident the first time you use your notebook to browse the Internet, stream music, and share files from a cozy hammock under the shade of a tree. RS

BY ANDREW LEIBMAN

How To Configure Windows 98 Or Windows 2000 On This Network

When you initially purchase your hardware, it's important to make sure it will be compatible with all of the operating systems you're planning to use in your network. You may need to visit the manufacturer's Web site to download a Windows 98- or Windows 2000-compatible driver for your particular wireless network adapter. To install the adapter, you'll need to follow the instructions that came with your hardware. Often this entails installing the device drivers prior to physically plugging a wireless network adapter into the PCI (Peripheral Component Interconnect) slot.

After installing your wireless network adapter on your computer, double-click its icon from the System Tray to launch the network adapter configuration utility. You can also access the utility by double-clicking the shortcut that appears on your Win98 or Win2000 Desktop after installing the driver software. This displays your network adapter's configuration options. Navigate through the configuration menu (layout and options vary by manufacturer) until you find a list of the available networks that your wireless adapter has detected. Select the SSID (Service Set Identifier) you established for your wireless network, enter and confirm the WEP (Wired Equivalent Privacy) or WPA (Wi-Fi Protected Access) encryption key, and then click Connect.

To share a folder in Win98, right-click the folder you want to share, click Sharing, click the Sharing tab, and then click the radio button in front of Shared As (in Win2000, the sharing option is labeled Share This Folder). Here you can change the Shared Name, and allow Read-Only or Full access rights. You can also set up a password from this dialog box. Click Apply and then click OK to close the dialog box.

To access the shared folders and drives from your Win2000 computer, simply double-click My Network Places from the Desktop and double-click the Computers Near Me icon. In Win98, double-click the Network Neighborhood folder from your Desktop. ❙

Nobody Home?

Whatever Happened to HomePNA?

The Home Phoneline Networking Alliance seemed to have a can't-miss technology. Does your house have a phone line? If so, a HomePNA-certified network card was all you needed to set up a home network. Now you can't find a single phoneline network device for sale at most major retail outlets. And all the big consumer networking manufacturers expired their products. What happened to phoneline networking?

HomePNA's Promise

The HomePNA concept was simple. Copper phone lines have plenty of unused capacity. Even between carrying voice calls and piping data through DSL (Digital Subscriber Line) connections, 99% of existing American households have sufficient capacity to carry network signals over the same wires.

HomePNA emerged around the time broadband Internet access became widespread and PC prices plummeted. People wanted to create home networks for sharing Internet.

Homes weren't wired for Ethernet, and running network cables from room to room wasn't feasible for most people. Rumors touted wireless networking as the next big thing, but HomePNA was here and now.

HomePNA wasn't without problems, however. Version 1.0, released in 1998, only supported 1Mbps (megabits per second) transfers. Having wires already in place was nice, but phone jacks weren't always handy for each PC. And although telephone wire can carry all the signals at once, it's still subject to electrical interference, which can necessitate special low-pass filters.

Boundless Optimism

Still, the future of HomePNA seemed bright just a few years ago. Rosy projections for growth in broadband Internet access had us all on high-speed connections in just a few years, driving up demand for home networking products. HomePNA 2.0, released late in 1999, increased speeds to 10Mbps. That's almost the same as Wi-Fi's 802.11b standard, and HomePNA promised better throughput than Wi-Fi's 3 to 4Mbps performance.

Top retail brands offered HomePNA products. The Alliance reported shipping two million units in the first quarter of 2000. Even better, HomePNA 3.0—promising 128Mbps and full backward compatibility—was planned for rollout in 2002. As long as the upgrades kept rolling out on time and the products got into people's hands, the possibilities were endless.

Rising Competition

Of course, the upgrades didn't roll out on time. Even worse, the products never caught on among the buying public. In the end, the Wi-Fi explosion was phoneline networking's death knell. Just as HomePNA 2.0 came out, wireless networking hit the airwaves. Despite slower speeds, questionable security, and potential interference from cordless phones, wireless' mobility and flexibility quickly caught consumers' attention. And Wi-Fi's ubiquity at coffee shops, hotels, and other public "hotspots" introduced the technology and drove demand for new products.

In the end, technology manufacturers turned their attention from finding innovative ways to create networks using the existing wiring in homes to promoting a networking technology with broader applicability and fewer limitations. In other words, Wi-Fi can do more with less—a fact not lost on cutthroat competitors.

Quiet Disappearance

After 2003, even after HomePNA 3.0's belated release, the technology began disappearing from store shelves everywhere. Manufacturers such as Linksys and D-Link quit making new products and stopped selling the ones they'd already developed. Network cards and gateways became harder to find, and press coverage became practically nonexistent.

But this shift points to the future. Despite its demise in the consumer marketplace, HomePNA hasn't gone away. HomePNA President Richard Nesin touts the technology's adoption by telecom companies and set-top box manufacturers as an example of its future potential. Providers are building HomePNA technology into their residential gateways and set-top boxes delivering next-generation IPTV (Internet Protocol Television) and DSL (Digital Subscriber Line). While you may not find products in the stores tomorrow, don't be surprised if next-generation multimedia devices for the wired home quietly rely on HomePNA. RS

BY GREGORY ANDERSON

A Network In Your Walls

Install A Powerline Home Network

Wireless networks are incredible—when they work. In a perfect environment they send a strong signal for hundreds of yards and operate at speeds comparable to that of most wired networks, but homes are far from the perfect environment. Signals must penetrate ducting, concrete, wood, and a variety of other obstacles, sometimes through several floors and sometimes at odd angles, and the result is that your home likely has several dead spots where a wireless signal simply won't reach.

You can also string Ethernet cable all over the house to create a speedy wired network, but why bother when there's already a network of wires installed throughout your house that can deliver network access to practically every room with equal strength? We're talking about your power lines, and using them for a home network is easier and faster than you may think.

The Pros & Cons Of Powerline Networks

Powerline networks only sound exotic because they are not used that often, but they work using the same principles that let the cable company send network data over cable lines and the phone company send network data over phone lines. Their key benefit is that they provide network access to every power outlet in your entire house. Just plug in the equipment, connect your computer or other network device to it, and you're set.

In the past, home powerline networking was excruciatingly slow, operating at 1Mbps (megabit per second) or even slower. The Linksys (www.linksys.com) hardware featured in this article won't set any network speed records, but still offers speeds of up to 14Mbps, while the hardware Netgear (www.netgear.com) submitted to us has an advertised top speed of 200Mbps, although we never achieved even half of that theoretical maximum. These speeds are adequate for streaming audio and most video files across a network, and also for light- to medium-duty file transfer operations. If you plan to use your network to frequently transfer multiple gigabytes of files between computers, a wired Ethernet setup is still your best bet, but modern powerline home networking equipment is a real step up from products of the past in terms of speed.

Unfortunately there is no way to prevent signals from traveling outside of your house and all of the way to the main transformer that sends electricity to your home, meaning that if you don't lock down your powerline network, other people connected to the same transformer can plug in some hardware and access your network. The chance of this is currently very low as so few people opt for powerline home networks, but all of the equipment discussed in this article encrypts everything that passes through it. Encryption scrambles all data flowing over the network so that even if someone does intercept it, they'll have no way of telling what it is.

Compatibility is another problem, thanks to competition between the HomePlug Powerline Alliance (www.homeplug.org), which champions the HomePlug standard, and the UPA (Universal Powerline Association; www.upaplc.org), which supports the vastly different UPA standard. The current version of UPA is up to twenty times faster than the older HomePlug 1.0 standard, and although most UPA devices will interoperate with HomePlug equipment, A UPA device's maximum speed is reduced to that of HomePlug (generally less than 20Mbps).

Buying Hardware

To install a powerline network, you need a router (also called an Internet Access Point or a gateway) that serves as the central point of the network and lets all of your networked components communicate with one another and share a broadband Internet connection. Your broadband modem plugs

Some powerline home network devices connect directly to a router or PC via their Ethernet port, shown here.

Other powerline network equipment connects to a computer using a USB port like the one on the front of this Linksys PLUSB10.

into the router's WAN (wide-area network) port using an Ethernet cable, and then you'll use another Ethernet cable to connect the powerline network's transmitter to one of the router ports. Never plug a powerline networking device into a power strip, extension cord, or UPS (uninterruptible power supply). Doing so can seriously degrade performance and may cause the device to stop working at all.

Most powerline network equipment comes in the form of an Ethernet bridge or a USB adapter, and we recommend using bridges whenever possible. They are easierto install and configure and work with a wider variety of equipment than adapters.

At minimum, creating a powerline home network requires one bridge that connects to the router via an Ethernet cable and at least one other bridge or adapter that plugs into an outlet somewhere else in your house and connects to a PC or other networked device via an Ethernet cable or USB cable. You'll also need one additional bridge or adapter for each additional device you want to add to the powerline home network.

There are products called switches (sometimes referred to as switched hubs) that can divide one Ethernet cable, such as that coming from a bridge, into several ports so that several network devices can share a single connection. Theoretically you could plug a powerline network bridge into the wall, attach its Ethernet cable to a switch, and then connect several devices in the same room to the switch's Ethernet ports, but read the instructions that came with your powerline network product carefully before doing so. Many manufacturers warn against using their products with a switch and in most cases there's no alternative to purchasing additional powerline bridges or adapters for each additional network device.

With the exception of Ethernet and USB cables, which are all generic and all work the same, purchase all of your powerline home network products from the same company (including your router, if possible). Sticking with a single manufacturer and a particular model means the products will work well together and can take advantage of any speed-boost and other features that manufacturer offers. It also lets you take care of troubleshooting with a call to a single company should trouble strike, and home networks are a magnet for trouble.

Now that the hardware is squared away, it's time to create a powerline home network. The following section is written for Windows XP users, although Windows 98 and Windows 2000 users can refer to the sidebars in this article for specific instructions regarding those operating systems.

Setup Tips: Linksys PLUSB10 PowerLine USB Adapter & PLEBR10 PowerLine Ethernet Bridge

Linksys offers a variety of HomePlug-based powerline networking products, and provided us with a pair of PLUSB10 PowerLine USB Adapters ($101) as well as a pair of PLEBR10 PowerLine Ethernet Bridges ($99.99) for testing. A powerline setup requires at least one PLEBR10, which is a bridge that attaches directly to an open Ethernet port on the router using an Ethernet cable. The unit then plugs into the wall and starts looking for other PowerLine devices.

The other equipment you'll need depends on how your devices connect to the network. If the device you want to add to the network connects via an Ethernet port, you need to use a PLEBR10 bridge. If the device you want to add connects to the network through a USB cable attached to an Ethernet adapter, then you need to use the PLUSB10. Both products come with all of the necessary connection cables, but they are only six feet long so you may need to purchase longer cables depending on how far your network hardware is from the wall socket.

When installing the PowerLine Ethernet Bridge, you can plug it into the wall and then connect it to a PC or the router before installing the included software. If you're installing a PowerLine USB Adapter, be sure to install the software first and then connect the hardware. To install the software for the USB Adapter, insert the included CD-ROM in your computer's CD or DVD drive, wait for the installation wizard to appear, and click Next.

Windows 98SE Setup Notes

Installing the Netgear hardware and the Linksys PowerLine Ethernet Bridge in Windows 98 Second Editon works exactly the same way as outlined for Windows XP, but the process for installing the Linksys Powerline USB hardware works a bit differently. You'll need your Win98SE operating system CD (the one that came with your computer or that you purchased for upgrading) because Win98SE will flash a warning asking for the disc during installation. Insert the disc when prompted, click OK, and if a Version Conflict message comes up click Yes. Finally, when the System Settings Change window appears, click Yes to reboot the computer and the hardware should work properly when Win98SE loads.

Netgear's newest powerline Ethernet technology is extremely fast and has a sleek design.

Agree to the terms of the license agreement, click Next, enter a user name, and select the Anyone Who Uses This Computer radio button before clicking Next. Click Install (refer to the sidebars for more information on what happens next if you use Win2000 or Win98SE), and when WinXP tells you the driver has not passed Windows Logo testing, click Continue Anyway. Click Finish and restart the computer.

When the software is installed, plug the adapter into a wall outlet, connect the adapter to your PC's USB port, and when the Found New Hardware Wizard appears, select the Install The Software Automatically radio button before clicking Next. The Windows Logo testing warning appears again, but click Continue Anyway to ignore it. Click Finish, and the adapter is now installed. You need to repeat this entire process for every machine connected to a powerline USB adapter, even if you move the adapter from PC to PC.

Installing the software for the Ethernet Bridge is much easier. Insert the CD in your PC's CD or DVD drive and click Setup when the Welcome screen appears. Click Next, click Finish, and click Yes to restart the PC. When Windows loads, you will see a PowerLine Configuration Utility icon on the Desktop. Double-click it, click Next, and the Device tab tells you what the current connection strength is. Select the Network tab and click Scan Network to find the other PowerLine devices on your network, and select the Security tab to change the default password from HomePlug to something else if you want to increase security. Just be aware that all powerline devices must have the same password to work with one another. Encryption is turned on by default, so you're good to go, but remember that you must repeat this entire process for every device connected to a powerline bridge.

Setup Tips: Netgear HDXB101 Powerline HD Ethernet Adapter Kit

Netgear's bridges use the UPA powerline standard that is capable of speeds up to 200Mbps, and its HDXB101 kit ($249.99) is the best way to set up a fast powerline network. The kit comes with two HDX101 bridges that are preconfigured to make installation as easy as possible. Just plug one of the bridges into a wall socket near your router and then connect the bridge to one of the router's numbered ports with an Ethernet cable. Next, plug the second bridge into any wall socket you like, connect it to a PC or other network device using an Ethernet cable, wait a minute until the bridge's blue light turns on, and you're finished. There isn't even a need to reboot the computer, and encryption is enabled by default. In our testing, speeds rarely exceeded 50Mbps, but that's fast enough to copy a few hundred average-sized digital music files over the network each minute.

Although setting up the HDX101 bridges is a snap, the package does come with software that you can use to change the default password to something more secure. Insert the included CD-ROM in the computer's CD or DVD drive, open My Computer, double-click the drive's icon, and click Install Software when the Smart Wizard appears. Double-click the NETGEAR HDX101 Configuration Utility icon that appears on the Desktop, select the Security tab, and change the Network ID to something other than PowerlineHD. You can then click Set All Devices to apply the new name to every HDX101 bridge on the network. Select the Main tab to select the operation mode (using all HDX101s on the network is optimal) and click the Scan button to see a list of all bridges installed on the network.

Don't Break The Bank

Because powerline network equipment is more expensive than wired Ethernet or even wireless Ethernet equipment, we recommend using it as a supplement to an existing home network. Stick an adapter in the basement if the wireless signal is bad down there, for example, but use less expensive wireless adapters (or even less expensive Ethernet cables) for your remaining devices. Also, check the manufacturer Web sites every month or so for firmware upgrades, which can enhance their performance, fix bugs, and add new features. There's nothing like getting a little speed boost for free every now and then. RS

BY TRACY BAKER

Windows 2000 Setup Notes

The setup process for the Netgear hardware and the Linksys PowerLine Ethernet Bridge under Windows 2000 is identical to the process for Windows XP. The only difference between Win2000 and WinXP when installing the Linksys PowerLine USB hardware comes during the initial software installation. After inserting the CD-ROM and clicking the Install button, Win2000 warns you that no digital signature was found. Ignore this notice by clicking Yes. Also, during the hardware installation, Win2000 should automatically detect that the PowerLine USB adapter is connected and once again display the Digital Signature Not Found warning. Click Yes again to ignore the message and the hardware installation should be complete.

Create A Hybrid Network

Make Your Wireless & Wired Networks Hold Hands

Your desktop computers are the pillars of your wired network. You enjoy being able to share your files, printer, and Internet connection among multiple computers over a reliable and consistent Ethernet link. Then, along comes a free-spirited notebook, making your life away from wires a breeze. But at the same time, that notebook presents a logistical nightmare when you consider how to connect it to your wired network wherever you happen to be using it.

Adding a wireless node (such as a notebook or Wi-Fi-capable PDA) to an existing wired network doesn't mean you have to scrap your cable infrastructure for a whole new wireless system, nor does it mean you have to gouge half a dozen holes in your walls to install new Ethernet cabling. You just need to create a hybrid network capable of handling both wired and wireless components. And you can do it yourself without ever having attended a single genetic biology class.

Add A Pinch Of Wireless

In most instances, your existing wired network consists of two or more computers networked with Ethernet patch cable and some form of central connecting device, such as a hub, router, or switch. If you're sharing your Internet connection, then you likely have another length of Ethernet cable connecting your DSL (Digital Subscriber Line) or cable modem to the WAN (wide-area network) port of your hub, router, or switch. To add wireless capabilities to this type of network, you can purchase either a wireless access point or a wireless router. The former acts as a central connecting device that lets your wireless and wired computers communicate with one another to share files and peripherals. Alternatively, a wireless router performs the same functions as a wireless access point, but also features routing and filtering capabilities.

If your wired network uses a length of crossover cable in lieu of a central connecting device, then you can add wireless capabilities by purchasing a wireless router and plugging the wired computers into the numbered LAN (local-area network) ports on the back of the wireless router. This also means you'll have to replace your crossover cable with a patch cable.

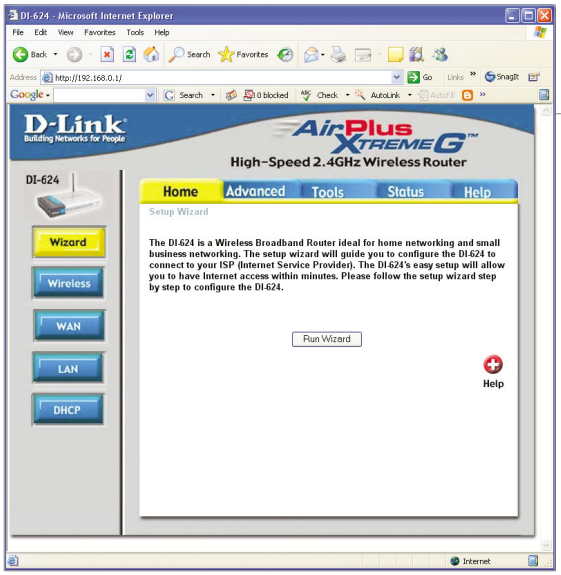
Most notebooks you'll find on sale today feature integrated wireless network adapters. You can add wireless functionality to older notebooks and desktops with a variety of wireless network adapters. External adapters come in USB and PC Card (Type II) formats, and internal adapters come in the form of PCI (Peripheral Component Interconnect) expansion cards.

Wi-Fi Dilemma

Depending on the placement of your wireless router, there are essentially two ways you can go about setting up your hybrid network. One configuration involves installing the wireless router in a central location so that it can broadcast its radio signals evenly throughout your home. The downside of this method is that you'll need to run a length of Ethernet cable between your wired router and the wireless router to maintain the network connection.

The other way involves replacing your existing wired router with a wireless router. Because the wireless router typically features four or more wired LAN ports, you can still maintain your wired infrastructure while accommodating wireless computers and devices. The drawback to this method is that the wireless router must be installed in about the same place as the old wired router. This arrangement is better suited for small to medium-sized homes and those in which the main computer (that is, the one connected to the wired router and DSL or cable modem) is in a roughly central location anyway.

Depending on the 802.11 wireless standard you choose to go with, radio signals are capable of passing through walls and multiple floors at distances of between 75 and 150 feet. For more information on the different 802.11 standards, see "Wires: Who Needs 'Em?" on page 32. And because one of the most common reasons for adding a wireless node to an existing wired


DI-624 - Microsoft Internet Explorer
D-Link
AirPlus XTREME G
High-Speed 2.4GHz Wireless Router
DI-624
Home
Advanced
Tools
Status
Help
Setup Wizard
Wizard
Wireless
WAN
LAN
DHCP
The DI-624 is a Wireless Broadband Router ideal for home networking and small business networking. The setup wizard will guide you to configure the DI-624 to connect to your ISP (Internet Service Provider). The DI-624's easy setup will allow you to have Internet access within minutes. Please follow the setup wizard step by step to configure the DI-624.
Run Wizard
Help

The configuration menu for your wireless router may look similar to this.

network is to forego the act of running extra Ethernet cable, this article will focus on replacing the wired router with a wireless one.

When purchasing hardware, make sure that it is compatible with all of the operating systems that exist in your network. Also, purchase wireless hardware that uses the same wireless standard to get the best performance bang for your buck.

Hybrid Engineering

We opted to use a D-Link AirPlus Xtreme G wireless router ($72; www.dlink.com) for our wireless network. Our existing wired network consisted of two computers and a shared Internet connection wired together with a router. All computers, including our wireless notebook, ran Windows XP Home Edition. When setting up your hardware, make sure you thoroughly read and follow the included instructions.

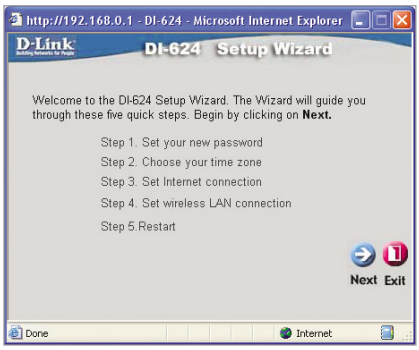
The first task is to configure the wireless router. Plug the wireless router's power adapter into a wall outlet near the main computer. It's best to use a centrally located computer, preferably close to the DSL or cable modem. Next remove the RJ-45 plug (which looks like an oversized phone plug) from the wired router's WAN port, and plug it into the WAN port of the new wireless router. Next, remove the RJ-45 plug that corresponds to the main computer from the wired router, and then plug it into the first numbered LAN port on the wireless router. Now both your main computer and your DSL or cable modem should be plugged into the wireless router via the WAN port and a LAN port respectively.

Consult the instructions to configure your wireless router. Typically this involves installing configuration software or using a Web browser to access the device's configuration menu. To configure our router, we'll follow the latter procedure. On the main computer, open a Web browser (such as Internet Explorer or Firefox) and then type the wireless router's static IP (Internet Protocol) address (as described in the router's manual) into the address field of the browser. The static IP address will look similar to http://192.168.0.1. Press ENTER to display the login prompt, type **admin** into the User Name field and leave the password field blank, and then click OK. You should see your router's main configuration menu. To launch the configuration wizard, click Run Wizard.

Click Next to display the Set Password screen, which lets you set up the login prompt password. Click Next, choose your time zone from the drop down box, and then click Next again. Depending on your connection type, the configuration software may automatically detect your WAN settings and skip the Select Internet Connection Type screen. If you're prompted to select a connection type, click the appropriate radio button and click Next to continue. If you're unsure which option to choose, check with your ISP (Internet service provider). If you chose Dynamic IP Address, you'll need to enter a host name or MAC (Media Access Control) address on the following screen. If you chose Static IP Address, then your ISP can provide you with the WAN IP Address, Subnet Mask, Gateway Address, and a Primary DNS Address to use on the following screen. If you chose PPPoE (Point-to-Point Protocol over Ethernet) and your ISP requires a username and password, the following screen lets you enter them. Your configuration wizard may display other Internet connection types, but these are the ones you're most likely to encounter.

The following screen lets you set your SSID (Service Set Identifier). Each wireless device that connects to your wireless router will use this name to identify your network. It's always a good idea to change the SSID from the default setting to provide an added layer of security. This screen also displays the current channel. After setting up your wireless router, you may notice slow connections speeds. This might be due to interference from other electronic devices that utilize that same channel. If your wireless router's configuration wizard allows it, you may be able to improve your connection speed by changing the channel to one that features less interference.

Some configuration wizards ask you to give the wireless router a unique name to distinguish it from other


http://192.168.0.1 - DI-624 - Microsoft Internet Explorer
D-Link
DI-624 Setup Wizard
Welcome to the DI-624 Setup Wizard. The Wizard will guide you through these five quick steps. Begin by clicking on Next.
Step 1. Set your new password
Step 2. Choose your time zone
Step 3. Set Internet connection
Step 4. Set wireless LAN connection
Step 5.Restart
Next
Exit
Done
Internet

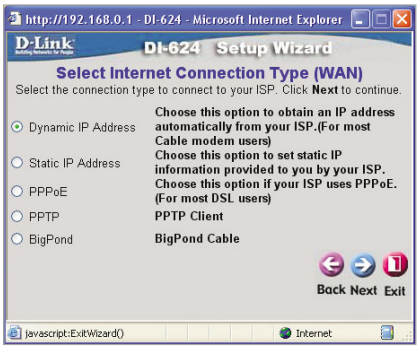
The Setup Wizard will walk you through the process of configuring your router to work on your existing network.

devices on the same network. Do so and then click Next. Typically, the final task is to enable your hardware's security features. All wireless networking hardware supports the WEP (Wired Equivalent Privacy) encryption scheme that secures data traveling over the network. Newer hardware also offers an improved version, called WPA (Wi-Fi Protected Access). Enable the highest level of encryption that your hardware supports, write down your encryption key, and then click Next. You may need to restart the wireless router to enable the changes.

Wi-Fi & Wires Wrap-Up

The next task in our hybrid upgrade is to connect the remaining wired computers to the new wireless router. Remove the RJ-45 plugs that connect to the remaining computers and plug them into the numbered LAN ports on the back of the wireless router. Because these computers were a part of the same workgroup when they were attached to the wired router, they should be able to communicate for file and Internet sharing right away.

To test your hybrid network, you can use a notebook with a wireless network adapter to connect to the wired PCs in your network. On your notebook, click Start, click Control Panel, click Network And Internet Connections (if you're viewing the Control Panel in Category View), and then click Network Connections. If you're viewing the Control Panel in Classic View, simply double-click Network Connections. Click the Wireless Network Connection icon, and then click the View Available Wireless Networks link on the left side of the window. Click the wireless network indicated by the SSID you chose when setting up the router, and then click Connect. Enter your encryption key, enter the key again to confirm it, and then click Connect. To access the other PCs on your network, click Start, click My Computer, and then click the My Network Places link from the left side of the window. Once you visit My Network Places for the first time, Windows puts an icon for it in your Start menu.


http://192.168.0.1 - DI-624 - Microsoft Internet Explorer
D-Link
DI-624 Setup Wizard
Select Internet Connection Type (WAN)
Select the connection type to connect to your ISP. Click Next to continue.
Dynamic IP Address
Choose this option to obtain an IP address automatically from your ISP.(For most Cable modem users)
Static IP Address
Choose this option to set static IP information provided to you by your ISP.
PPPoE
Choose this option if your ISP uses PPPoE. (For most DSL users)
PPTP
PPTP Client
BigPond
BigPond Cable
Back Next Exit
javascript:ExitWizard()
Internet

You may need to consult your ISP to determine your Internet connection type.

To give the PCs in your network access to your notebook's files, click the Set Up A Home Or Small Office Network link from the left side of the Network Connections window. Click Next, click Next again, click the checkbox in front of Ignore Disconnected Network Hardware, and then click Next. Click the radio button in front of This Computer Connects To The Internet Through A Residential Gateway Or Through Another Computer On My Network, and click Next. Input a PC description and a unique PC name, and then click Next. On the following screen, enter the network's workgroup name. Click Next, click the radio button in front of Turn On File And Printer Sharing, click Next, and click Next again. Click the radio button in front of Just Finish The Wizard, click Next, click Finish, and then click the Yes button to restart your PC.

Get Around

Upgrading your existing network to accept wireless devices is a simple task. Once completed, your new hybrid network lets you use a notebook or PDA to access files and browse the Internet from a lot of new places. Now you just have to worry about losing your device between the sofa cushions. RS

BY ANDREW LEIBMAN

How To Configure Windows 98 Or Windows 2000 On This Network

If you're using an older notebook or PC that uses either Windows 98/2000, then you'll likely need to install a wireless network adapter. Make sure the adapter you purchase is compatible with the system's operating system and use the appropriate driver version. Install the drivers, and then insert the wireless network adapter using its interface method (USB, PC Card, or internal expansion card). Click the adapter's icon from the System Tray to launch the connection utility. If the wireless network adapter's icon doesn't appear in the System Tray, double-click the icon for the configuration utility from your Desktop. You will see a list of detected networks. The connection utilities vary by manufacturer, but you should be able to select your network from a list. Enter and confirm the WEP (Wired Equivalent Privacy) or WPA (Wi-Fi Protected Access) encryption key that you established, and then click Connect.

To share a folder or hard drive on your notebook or PC, right click the item, and then click Sharing. In Win98, click the radio button in front of Shared As (in Win2000, this option is called Share This Folder). This dialog box lets you change the Shared Name and access rights for the other computers on your network. Click Apply and then click OK to close the dialog box.

To access the shared folders and drives from your Win98 system, double-click the Network Neighborhood folder from your Desktop. In Win2000, simply double-click My Network Places from the Desktop and double-click the Computers Near Me icon.

Your Networked Media Center PC

Entertainment On The Line

Now that you have your home network up and running, the next step is to give it something to do besides provide Internet access to all your computers and make it possible for them to share files. These things are important, certainly, but there's so much more you can do with your LAN (local-area network), especially if you connect a MCPC (Windows XP Media Center PC) to it. With everything from media streaming to network storage, and control of a huge number of add-on devices, MCPCs can enhance your network significantly.

Turn Your PC Into A Network Storage Device

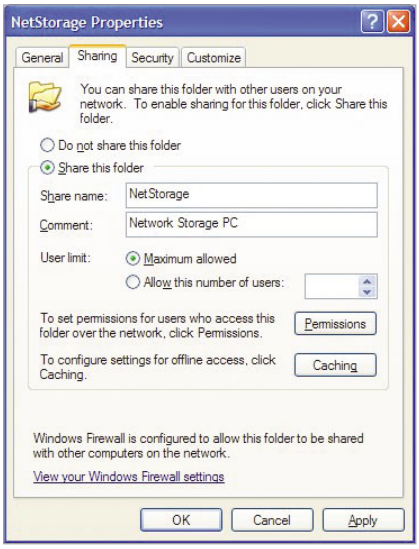
Why do you need a network storage device? Security and convenience, of course. First, you can store data from all your networked PC users in a safe place: a hard drive that isn't part of the machines on which those data files were created in the first place. While on the network storage device, that data can be backed up regularly without disturbing the other users (backup software always slows things down), and if the transfer to the storage device is handled automatically, there's almost no chance at all that files will be lost, even if the user's PC goes belly-up.

Second, the stored data is accessible from anywhere on the network. Now, you can certainly set up your PCs to share folders among each other, but in order to access those PCs, they have to be turned on. With a network storage system, only that device needs to be on. The result is greater convenience, of course, an important consideration when file access is a major focus of your household's entertainment life.

Which brings us back to the Media Center PC. The conventional wisdom is that network storage devices can be nothing more than older PCs outfitted with a new hard drive and left powered on all the time, or at least during the periods of time when users are most likely to want access. Its role as a PC isn't important, only its role as a remote hard drive. However, the MCPCs have an attraction as storage devices for exactly the opposite reason. Not only can the MCPC act as a typical storage device, it can also be the household's entertainment center. As users download video or music files, they can automatically store them onto the MCPC and provide instant access to them for playback. In other words, instead of using a PC as safety device that you keep out of the

way, your housemates use it as a central reservoir for all your digital entertainment activities, feeding it with material for everyone's benefit.

The first step in turning your MCPC into a network storage device is to provide a folder on that PC that all the users on your network can access. Ideally, however, you'll provide more than a folder, instead providing a separate large hard drive. You'll need a large drive to accommodate the size of audio and especially video files, and having two drives will allow you a much more secure backup system (it's always best not to back up data to a drive on which your local data and operating system are stored). However, whether or not you provide a separate hard drive, you should never share the whole drive anyway, in case you decide at some point to use that drive for local storage not suitable for sharing. For this demonstration, we'll share a single folder.


NetStorage Properties
General
Sharing
Security
Customize
You can share this folder with other users on your network. To enable sharing for this folder, click Share this folder.
Do not share this folder
Share this folder
Share name:
NetStorage
Comment:
Network Storage PC
User limit:
Maximum allowed
Allow this number of users:
To set permissions for users who access this folder over the network, click Permissions.
Permissions
To configure settings for offline access, click Caching.
Caching
Windows Firewall is configured to allow this folder to be shared with other computers on the network.
View your Windows Firewall settings
OK
Cancel
Apply

When you share your media storage folder on a network, be sure to set a maximum number of users that can access it at once.

Hauppauge's Wireless MediaMVP is an easy way to connect your media PC to your home entertainment center.

Open My Computer, double-click the icon for the hard drive on which you want to store and share the network files, right-click an empty area of the folder's window and choose New, then Folder. Name the folder whatever you like (we've chosen "NetStorage").

To organize the shared files more efficiently, double-click your new folder and create several subfolders. Name each one so that your users will know to share data of a particular type there. For example, you could set up folders called "Video Files", "Audio Files", "Data Files", "Game Files", and "Other Files". Obviously, you can subdivide these into as many categories as you need.

Share Your Fun

With the folders created, you can now share them. Right-click each folder's icon and choose Properties, then choose the Sharing tab. Click the Share This Folder radio button and type an easily recognizable name in the Share Name field (Windows automatically fills this in with the name of the folder itself). In the User Limit area, specify if you want to restrict the number of simultaneous accesses. You might as well restrict it to the number of users on the network. Click OK, and the folders are shared, as indicated by the hand icon that appears under the folder icons.

The folders are now shared, but that doesn't mean network users have access to them. First, you have to create accounts for them on the MCPC, so that they can log in to the network folders. These accounts are independent of whatever accounts are on their own PCs, but be careful: If you give them the same username and password as they have on their own Windows PCs, logging into their local machines will also give them access to the network folders. As a result, you should assign different usernames and passwords to prevent unwanted access by others who might use their PCs (friends, for example).

To create accounts on the Media Center PC, open Control Panel and double-click the User Accounts icon. Choose Create A New Account from the resulting screen and give the account a name; presumably the user's name, but it's your choice entirely. Click Next and ensure that each account is of the Limited type, not the Administrator type. Click Create Account to establish it, then double-click the icon for this account from the resulting User Accounts screen. Click the Create A Password link, fill in the required fields to establish a password for that user, and click Create Password. Follow the same procedure for as many accounts as you need, then inform your users of their username/password combinations.

Now the PC is ready for its new function as an entertainment network storage device. When users log on to their own machines, they open My Computer and click My Network Places, where they should see the shared folders you've created; if not, they must click the View Workgroup Computers link on the left and then double-click the icon for the MCPC. When they double-click the icon for one of the shared folders, Windows prompts them for

The ShowCenter 200 from Pinnacle Systems supports nearly all the media formats you'll need.

their username/password. Once they've done so, they can save files directly into those folders or copy and move them using My Computer or Windows Explorer. They can also access those folders and copy files to their local PCs or open files directly from the MCPC.

Be sure to configure the Media Center PC to automatically refresh its list of media files, configuring it to look specifically in your new folders for these updates. That way, the pictures, music, and videos will be available to anyone using the MCPC interface on your connected TV.

Of course, with your network drive in place, it makes sense both to back up its data regularly and, in turn, to have your users back up their PC's data to it. Create a folder for each user's backup needs, then purchase a good data backup program and install it on the networked PCs. Windows' own backup utility, which bears the truly unpretentious name Backup Utility, can do the job for you, but establishing a connection to a network drive can be difficult, and it's not exactly feature-rich. Programs such as Genie Backup Manager Home 7.0 ($49.95 single user; www.genie-soft.com) and Roxio's Backup My PC 2006 ($49.99; www.roxio.com) offer far more features and stronger backup automation.

Extend Your Media Center PC

There's one main problem with using Windows XP Media Center: It can be a little inconvenient to have one sitting beside the entertainment center in your family room. Of course, the entire purpose of the Media Center is to provide a central point for stored entertainment files, so if you can't have it right by the TV, either because it's too noisy or too big, what do you do? One option is to use a notebook that's running Media Center as its operating system, but notebooks are expensive and eventually someone will pick it up and take it to school, to the office, or on a trip. And if your desktop (or notebook) MCPC is your main computer, and they're certainly powerful enough to be so, you want to be able to use it away from the family room. Fortunately, products have become available that let you extend your MCPC so that you can place the PC at a distance from the entertainment center itself.

Send your audio files across your home entertainment network with the Slim Devices Squeezebox.

One example is the Hauppauge Wireless MediaMVP ($149; www.hauppauge.com), which streams MP3 or WMA (Windows Media Audio) audio files and MPEG-1, MPEG-2, and DivX video files from your MPCP to your entertainment center via your 802.11g wireless network. To install it, you position the MediaMVP near your TV and audio system, add it to the network by setting the wireless configuration to match that of your current access point (although MediaMVP can find your access point on its own), and connect the audio and video cables to your entertainment devices (composite and S-Video outputs are included for video, standard RCA for audio). You then configure it to find your audio, video, and graphics files on your network and control your selections via the included software and remote control.

A similar product is the Pinnacle Systems ShowCenter 200 ($299; www.pinnaclesys.com). Setup is almost identical to the Hauppauge unit, but the ShowCenter offers an expanded range of technology. In addition to the MediaMVP's outputs, it also has component video and optical audio outputs, and it plays MPEG-1, MPEG-2, MPEG-4, Xvid, and Windows Media Video 9 files. Through its software you can categorize media into playlists and albums and sort your audio by genre.

Microsoft offers a Media Center Extender product of its own, but you need an Xbox 360 gaming console to use it. To install it, you connect the Xbox 360 to your wireless network and to your TV, then fire up the Xbox's configuration screens and choose the Media Center menu item. As long as your MPCP has the Update Rollup 2 installed (you can download it from the Microsoft site at no cost), the Xbox connects to the MCPC and works with its settings and its interface, allowing you to control your MCPC using your Media Center remote control. There are two drawbacks to such a system, however. First, you need an Xbox 360, which

costs nearly $400, more than most wireless media extenders. Second, when you're using the Xbox as an extender, nobody can use it to play video games.

Other products let you stream audio-only. One of the more popular is Slim Devices' Squeezebox ($249; www.slimdevices.com), which connects to your network through its built-in 802.11g adapter and then to your audio system via standard RCA cables or, for better quality, digital optical or digital coax connectors. The Squeezebox streams CDs and other lossless formats (Apple, FLAC, and WMA lossless), and uncompressed WAV and PCM (Pulse Code Modulation) formats. It also handles MP3 and WMA files at all data rates. In addition, it works with AAC and Ogg Vorbis files, among others. The company's SqueezeNetwork gives you access to a huge variety of radio streams as well. And if you're really serious about your music, the company's Transporter ($1,999) device promises audio streams of exceptional professional quality.

We're also starting to see Wi-Fi-enabled speaker systems come onto the market. One of the most intriguing wireless speaker product lines is from Australia's Avega Systems (www.avegasystems.com), who promise a range of kits ranging from two-speaker to seven-speaker systems. These will stream audio data directly from the wireless network to the speaker itself. No prices have been announced as of yet, but they're likely to be pricey. Of course, wireless speakers have been available for several years now, but only those using FM technology, not Wi-Fi technology, with a resulting loss of both quality and capabilities.

Windows XP Media Center is an operating system designed for extensibility. It assumes the existence of an external entertainment center, or at least an external TV, and it has built-in capabilities to feed entertainment files to your devices. Given this design emphasis, it makes perfect sense to extend it further by attaching it to a wireless LAN and having it connect to an entire range of devices using the convenience of Wi-Fi. In fact, as devices that can become part of a Media Center configuration become more and more plentiful, such extensions will almost certainly become essential, with your MCPC becoming an increasingly important part of your household's computing environment. RS

BY NEIL RANDALL

Connect Your TiVo

If you own a TiVo, you can connect it to your wireless network using the TiVo's built-in support for Wi-Fi. The main reason to do so is that it gives you the option of displaying TiVo output on any computer or TV on the network. The secondary reason—although primary for some TiVo users, certainly—is that you can connect to the TiVo network via your Internet connection instead of over the phone, saving considerable time with program schedules. You can also use the network for TiVo ToGo transfers to any connected device, including portable media players such as an iPod or a Palm Treo.

The first thing you need, other than a wireless network, is a wireless adapter for the TiVo. While any 802.11b USB adapter will do, TiVo has made some noises about providing support for 802.11g, so you'd be wise to purchase one of those instead. TiVo offers one, in fact, and it's proven popular because of its ease of connection and its speed. The TiVo Wireless G USB Network Adapter for Series 2 DVR (a.k.a. the AG0100) is available from Amazon.com (www.amazon.com) for $49.99, an entirely reasonable price for any 802.11g adapter.

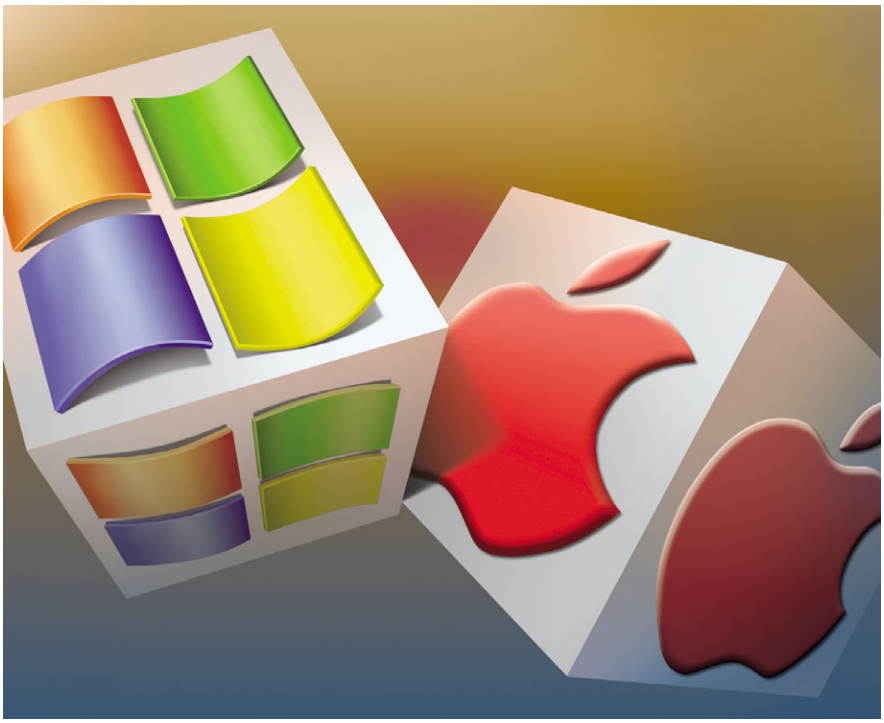
To install the adapter, plug the USB cable into the TiVo's USB port and then call up the TiVo's Phone and Network Setup screen from TiVo Central (via TiVo Messages and Setup). Choose the Change Connection Type item and then Edit Phone Or Network Settings. From that point on, it's a matter of following the instructions on the screen, proceeding into the Wireless Settings area and connecting to the network's name. If your wireless network uses WEP (Wired Equivalent Privacy) security, you'll need to enter the supplied WEP password using the alpha-numeric option, and depending on the configuration of your access point, you might need to input information in the TCP/IP (Transmission Control Protocol/Internet Protocol) setup area.

After you've provided all this, TiVo establishes the connection and provides information about the signal strength. In any wireless media transfer, signal strength is absolutely key, so use the signal strength information to place the adapter in the best possible position, trying a variety of locations until the signal strength is maximized.

If you're using a third-party USB adapter, you'll follow precisely the same process. The difference is that TiVo might not find the network quite as easily. Of course, in order to adjust the wireless settings you need to know what they are in the first place, so call up your router's configuration dialog on your PC before you start and write down all the required information: SSID (Service Set Identifier), channel number, WEP password, etc. ▌

Across The Great Divide

Combine Macs & PCs On A Single Network



We've all seen them break out: arguments among computer users over the merits of one's platform of choice and the shortcomings of the other guy's.

User allegiances aside, PCs and Macs have coexisted peacefully for years. Files created in Microsoft Office, for instance, usually flow between platforms without a snag. Graphics and audio files don't care if they're opened in a Windows or Mac application.

Although millions of users have never forced any greater mingling of the species than transferring files by email or removable media, PCs and Macs can communicate much more directly than that. It comes down to the operating systems. What we have in Windows XP and Mac OS X are two mature operating systems that have decided to be grown-ups about the whole business and admit that it really is better if you play nice with whoever's next to you.

This friendliness is due mainly to the use of open standards in both systems, and OS X itself, which has throughout its existence incorporated Windows networking protocols and supported Windows file formats.

So What Can They Do Together?

From a marketing standpoint, Apple trumpets cross-platform networking compatibility more prominently than Microsoft does . . . but then, as a minority platform, Apple has to.

For a more thorough overview of the networking potential than we have room for here, as well as some of the technologies and standards involved, visit Apple's Windows page (www.apple.com/macosx/features/windows). Look for the Technology Brief box, where you'll find a downloadable 12-page PDF file that should tell you as much as you want to know.

In a nutshell, though, as long as PCs and Macs are connected to a network either by Ethernet cable or a Wi-Fi wireless standard (802.11b/g), and have reasonably up-to-date operating systems (more on that in a moment), then they should have no trouble sharing files and connected printers. And it shouldn't matter if you're adding a Mac to a group of PCs, a PC to a group of Macs, or mixing them in more or less equal numbers. Where it counts, they'll still speak the same language.

Also, by installing Microsoft's Remote Desktop Connection Client 1.0.3 for Mac (www.microsoft.com/mac), it's even possible to control a Windows PC from a Mac Desktop. The PC Desktop is displayed inside a window on the Mac. There is, unfortunately, no free resource for controlling a Mac from a PC. This would take a third-party program such as Timbuktu Pro (starting at $89.95; www.netopia.com).

One warning, though: For file sharing, it's best to restrict the shared resources to folders, although it's no problem if hierarchies of additional folders are nested inside. Attempting to make one machine's entire hard drive available to the other platform can result in unreliable behavior.

In Preparation

Assumptions can be dangerous, but we're still going to make a couple here.

First, we're assuming that you've already set up your network and have successfully added your computers to

it by cabling them to a hardware hub, linking to a wireless router, and so on. If not, this probably isn't the place to learn about initially setting up a network. We cover that topic elsewhere in this issue, so see "Getting Wired & Going Wild" on page 27 and "Wires: Who Needs 'Em?" on page 32.

However, if you have just one of each breed, your network can be as simple and direct as a PC and a Mac connected by a single Ethernet cable.

Second, we're assuming that you have the latest operating systems for both platforms. There's definitely been enough time to keep current. WinXP's last major update, Service Pack 2, was issued in August 2004. Mac OS X 10.4, nicknamed Tiger, was released in April 2005. Apple has refined OS X's cross-platform networking capability with each new version, and while it's still not perfect, it's improved steadily.

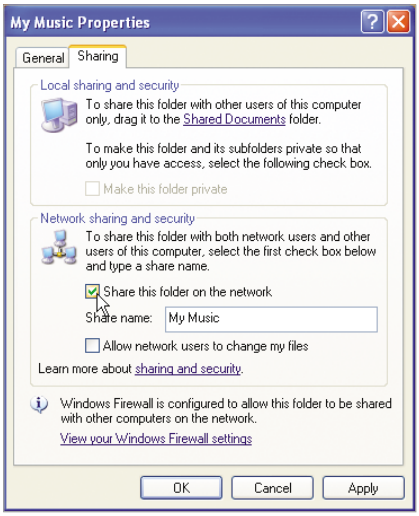
Even if you're behind on your upgrades, the instructions given here should apply to earlier system versions, too, although minor discrepancies may crop up.

As we go to press, major new versions of both operating systems—Windows Vista and Mac OS X 10.5, nicknamed Leopard—are scheduled for release in, respectively, early 2007 and late 2006. It remains to be seen how that will affect the instructions given here, but it's reasonable to expect that networking the two platforms will be smoother yet . . . at least after a round or two of bug fixes.

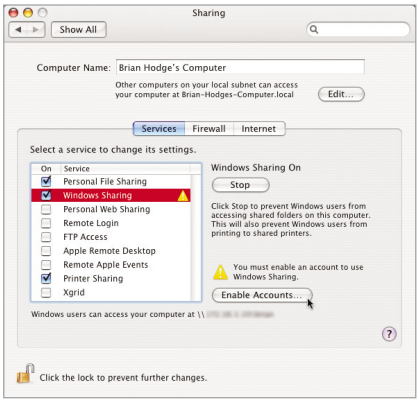
Cross-Platform File Sharing

The sharing, editing, and transferring of files between computers is, for most users, the main reason for networking. Thanks to an open-source technology called Samba, Macs and PCs can access one another's files almost as easily as two machines on the same platform.

The main wrinkle is that you need to manually configure the machines to point them toward each other. This can initially present a stumbling block to Windows users accustomed to the auto-detection that occurs when different PCs are connected to the same network, particularly under Windows XP Professional, which is tailor-made for networking.


My Music Properties
General
Sharing
Local sharing and security
To share this folder with other users of this computer only, drag it to the Shared Documents folder.
To make this folder and its subfolders private so that only you have access, select the following check box.
Make this folder private
Network sharing and security
To share this folder with both network users and other users of this computer, select the first check box below and type a share name.
Share this folder on the network
Share name:
My Music
Allow network users to change my files
Learn more about sharing and security.
Windows Firewall is configured to allow this folder to be shared with other computers on the network.
View your Windows Firewall settings
OK
Cancel
Apply

In Windows XP, use the Properties dialog's Sharing tab to enable folders for sharing.



In Mac OS X, the System Preferences Sharing pane is where you'll activate sharing for files, Windows, and printers.

The instructions below apply to linking one Mac and one PC. You'll need to repeat the procedure for as many machines as you want to network with one another.

Start with pen and paper. Before instructing the pair to talk to each other, gather a few tidbits of information you'll need:

The **Workgroup** that the PC belongs to. To find it, right-click My Computer, choose Properties, and click the Computer Name tab. The default name is MSHOME.

The PC's **IP (Internet Protocol) Address.** Click Start and select Run. Type **cmd** and click OK. In the new window, type **ipconfig** and press RETURN to get the IP information.

The Mac's **IP Address.** Click the Apple menu, select About This Mac, and click More Info. Click Network in the left-side list.

The **Short Name** for the Mac's user account. Open System Preferences from the Apple menu. In the System group, click Accounts.

The user account **Passwords** for each computer. (If you're using Windows XP Home and haven't set it up with password protection, you'll need to do so before proceeding.)

Configure the PC. Because it's better to restrict file sharing to folders, decide which existing folders you want to share, or make a new folder specifically for sharing with the Mac.

Now right-click a folder and select Sharing And Securities. (You can also choose equivalent commands in the Windows Explorer task pane, if you haven't disabled it.) In the Properties dialog box, activate the checkbox for Share This Folder On The Network. If the folder's existing Share Name is lengthy, it's better to revise it to something short and simple, without spaces—"macshare," for example. Another checkbox will allow network users to change the shared files.

Configure the Mac. First, add the Mac to your Windows workgroup. Go to the Applications folder, then the Utilities folder, and launch Directory Access. Click the padlock to enable changes, if necessary, and supply the password. Select SMB/CIFS (activate the checkbox if it isn't already), then click Configure. Enter the workgroup name and click OK.

Next, enable sharing by opening System Preferences. Under the Internet & Network group, click Sharing. Click the padlock to enable changes if necessary. Under the Services list,

activate the checkboxes for Personal File Sharing and Windows Sharing. Click Enable Accounts and, in the list that appears, click the checkbox beside the user account name; this makes the account's home folder visible to PCs.

Connect from the PC to the Mac. Open My Computer, then My Network Places. Click Add A Network Place; this launches the Add Network Place wizard. Click Next.

Now select Choose Another Network Location and click Next. Enter

Add Network Place Wizard
What is the address of this network place?
Type the address of the Web site, FTP site, or network location that this shortcut will open.
Internet or network address:
\\192.168.1.10\robbie
Browse...
View some examples

To establish a network connection between a Mac and a PC, it's imperative to use their IP (Internet Protocol) addresses to point them toward each other.

the Mac's IP address and the account's short name into the data field in this format:

\\IP Address\short name

With the actual address, it will look similar to this:

\\192.168.1.10\robbie

Click Next, then give the Mac location an easier name for future reference. Click Next, and that completes the wizard.

Now, in My Network Places, you'll find a new folder with the name you've just supplied. This is your access to the Mac user's home folder; inside are separate folders for documents, music, photos, etc.

Connect from the Mac to the PC. With the Finder as the active application, click Go in the menu bar and, from the drop-down menu, select Connect To Server. Enter the PC's IP address in this format:

smb://IP Address

With the actual address, it will look similar to this:

smb://192.168.1.10

To add the address to the Favorite Servers list, click the plus (+) button. Now click the Connect button. When the connection is established, a pop-up menu will appear so you can choose which of the shared folders on the PC you want to connect to. Click OK.

Next, fill in the PC's workgroup name, plus the username and password for the Windows account. If you check the box for Remember This Password In My Keychain, the Mac will auto-fill the password whenever you establish the connection in the future. Click OK, and the PC's shared folder will mount on the Mac Desktop.

If you only have a single PC folder you want to share with the Mac, there's a slightly more direct path bypassing the pop-up menu. After choosing Connect To Server, enter the PC's IP address and the name of the folder you're after. It will look similar to this:

smb://192.168.1.10/macshare

Click Connect, and that will take you directly to the same authentication step described above.

Cross-Platform Printer Sharing

In most small networks, most users want to share printers, which takes just a few adjustments beyond the file sharing you've just enabled.

Share a Windows printer with a Mac. To permit network access to a printer connected to a PC, click Start and select Printers And Faxes. Or, click Control Panel, Printers and Other Hardware, and then Printers and Faxes. Right-click the printer and select Sharing. In the Properties dialog box, click the Share This Printer radio button. If you desire, revise the name in the Share Name field, then click OK.

To ensure that the printer is available under Mac OS X, go to the Applications folder, then Utilities, and launch Printer Setup Utility. Click Add, which opens the Printer Browser. Select the PC-connected printer in the list and click Add.

Share a Mac printer with Windows. To permit network access to a printer connected to a Mac, open System Preferences from the Apple menu and select Sharing. Under the Services tab, activate the Printer Sharing checkbox. If you have multiple printers connected and want to exempt some units from sharing, go to the System Preferences' main view and, in the Hardware group, select Print And Fax. Click the Sharing tab and deactivate the checkboxes for the printers you don't want to share.

To ensure that the printer is available in Windows, click Start and select Printers And Faxes. Under Printer Tasks, click Add A Printer and click the wizard's Next button. Click the second radio button (A Network Printer . . .) and click Next to locate and select the printer by browsing for it.

One Big Happy Family

If you encounter any connectivity problems, it may be due to a firewall. Although PC firewalls generally have no trouble passing traffic from the network's Windows machines, some third-party firewalls may block connection attempts from a Mac. If this happens, add the Mac's IP Address to the firewall's trusted sources.

On the Mac, OS X is secure enough that the built-in firewall provides sufficient protection, and it should reflect your Services settings. However, if you need to verify anything, open the System Preferences' Sharing pane, click the Firewall tab, and you'll see the types of communications currently permitted.

Macs and PCs may be rivals, but when there's work to be done, they can put aside their differences. With a few settings in place, you can make them talk to each other like old friends. RS

BY BRIAN HODGE

Peripheral Fun

Networking With Miscellaneous Devices

If you have a home network, you might wonder how to get the most out of your investment. The benefits of networking your computers are many—you can share a printer, share an Internet connection, and share files. But what about the TiVo or your iPod? How can you connect multimedia devices to your home network for even more functionality?

Thankfully, home entertainment devices and home networks are offering up more and more interoperability and support for each other. Here we'll discuss how to attach a variety of devices to your wired Ethernet or wireless home network. Before we get to the nitty-gritty, let's discuss a few universal topics that will get you started off right.

Before You Begin

Because wired and wireless networking is a standardized process, there are a number of caveats that apply, no matter what type of device you want to connect. Here's a rundown of important points to consider.

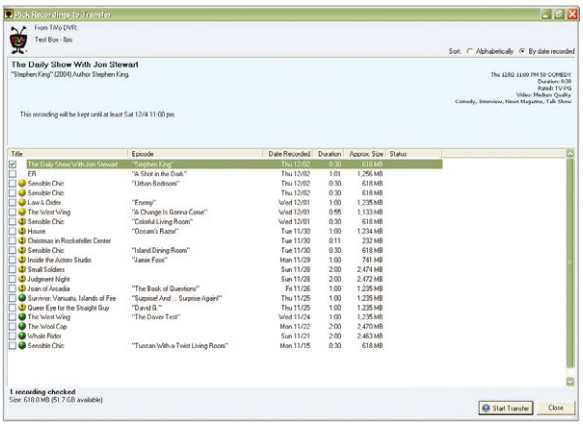
Wired networks. The main challenge with connecting devices to a wired network is the cable. If your home is like most, your computers are not located next to your television or stereo equipment. You can string a single Ethernet cable up to about 300 feet, but if you need to run it even longer, you'll need a repeater to extend the cable's range.

Other than running cable, connecting a device to a wired network is considerably less complex than connecting it to a wireless network. And if you don't mind dealing with cable between rooms, wired network connections are also less likely to succumb to interference and other connection problems. Speed is another factor to consider. For example, transferring video requires a lot of bandwidth. TiVo recommends using wired over wireless networking for faster transfer speeds with today's technologies. Wired networks can transfer data at up to 1Gbps (gigabits per second), whereas most current wireless technologies are limited to about 54Mbps (megabits per second) or less.

Wireless networks. If your home network is wireless, you should know the type of wireless technology it supports (typically 802.11a, 802.11b, or 802.11g). Note that 802.11g wireless APs (access points) work with 802.11b wireless devices.

You should also know the wireless security method your network uses and the accompanying passphrase, which are available in the wireless AP administration interface. The three security encryption methods used today are WEP (Wired Equivalent Privacy), WPA (Wi-Fi Protected Access), and WPA2 (Wi-Fi Protected Access 2). Of these, WEP is the least secure. WPA and WPA2 are more secure and are preferred for wireless networks.

Newer wireless APs and Windows XP systems support WPA and WPA2, but some multimedia devices offer WEP only. If you don't want to lower the overall security of your network,



TiVoToGo lets you transfer videos between networked computers and the TiVo Series2 DVR (digital video recorder).

The D-Link DSM-520 MediaLounge is a multimedia center powerhouse that supports numerous multimedia files, Internet radio, protected Windows audio files, and HD video and photos.

consider using a wireless AP that includes wired connectivity, such as the Linksys WRT54G Broadband Router ($69.99; www.linksys.com), so you can use the AP's wired connection for the multimedia device. Alternatively, some wireless APs support a mix of encryption technologies.

Regarding signal range, wireless multimedia devices cannot be more than 300 feet (preferably 100 feet) from the wireless AP. For best signal strength, fully extend the multimedia device's wireless antenna (if applicable) and locate it away from power supplies and other electronics that may interfere with the signal (microwaves or cordless phones, for example). If your device cannot connect to the wireless network, you may need to install a wireless signal booster.

Finally, many multimedia devices don't come with built-in wireless networking. If the device has a USB port, you can often add the device to a wireless network with a wireless USB adapter. Some devices offer specialized adapters designed for the device, and others may work with a computer-style adapter.

Connect A DVR

Connecting a DVR (digital video recorder), such as a TiVo Series2 DVR (www.tivo.com), to your home network gives you more options for digital video. With TiVoToGo and the free TiVo Desktop software, for example, you can transfer videos among computers on the network and the DVR. If you have multiple DVRs, you can transfer videos among them, as well. And if you have a video-capable portable device, such as a Sony PSP, Apple iPod, or Palm Treo, TiVoToGo can download files to it.

In addition to more video playback options, connecting a DVR to your home network can also provide your networked PCs with access to digital music and photos. With TiVo, for example, the TiVo DigitalMusic Player accesses a networked computer's digital music collection. Using the TiVo remote and your television screen, the player lets you select music to play, create playlists, and shuffle your tunes to play through your home entertainment system. The TiVo DigitalPhoto Viewer displays pictures from your computer on your television screen. It supports slideshows, photo albums, and photo searching.

Wired networks. Some DVRs, including TiVo Series2 DT (dual tuner) devices, provide a built-in Ethernet connection. For those that don't, there are Ethernet adapters that plug into a USB port on the DVR. Check the DVR manufacturer's requirements and verify that a particular Ethernet adapter is compatible with your DVR before you buy one. You also need an Ethernet cable long enough to reach the DVR from the network router.

To configure a multimedia device on a wired network, connect the Ethernet adapter (if applicable) to the DVR. Next, connect one end of an Ethernet cable to the DVR's Ethernet adapter and connect the other end to the network router. Follow the DVR manufacturer's instructions to configure the network connection, if necessary. (The connection may configure itself automatically.) Test the DVR's network connectivity to ensure the DVR is communicating with the wired network.

Wireless networks. If you decide to wirelessly connect the DVR to your network, you will probably need a DVR-compatible wireless adapter. Most DVRs do not come with built-in wireless capabilities. When purchasing an adapter, make sure it supports the same Wi-Fi standard as your wireless AP, usually 802.11b or 802.11b/g. You may also need to purchase a USB cable to connect the adapter to the DVR.

TiVo users can purchase the TiVo Wireless G USB Network Adapter ($59.99; www.tivo.com) for TiVo Series2 devices. TiVo states that the adapter optimizes wireless performance, and that it supports WEP encryption. (According to TiVo customer support, more secure WPA encryption will be added through a software update in the future.)

To configure your wireless DVR connection, connect the wireless adapter to the DVR using a USB cable. Next, configure the DVR to recognize and connect to the wireless network. To do this, you'll need to know the wireless network's SSID (service set identifier), the type of security encryption it uses (WEP, WPA, or WPA2) and the encryption key passphrase. After you enter the network information into the DVR, test its wireless network connectivity to ensure it's communicating with the wireless network.

Connect Multimedia Devices

Devices that distribute digital media from your home network to

your home entertainment system are evolving and improving. And other devices, such as the Microsoft Xbox 360, are adding multimedia network support to their collection of capabilities. Here we give you details about connecting a variety of multimedia devices to your home network.

Slingbox. The Slingbox from Sling Media ($199; www.slingmedia.com) shifts your television viewing from a TV to your Windows-based PCs and mobile devices. With a high-speed Internet connection, you can even watch TV in a remote location. Slingbox streams the video through the Internet to your Windows PC or mobile device with the proprietary SlingPlayer software.

To bridge your home entertainment system with your computer or Windows mobile device, you must have a wired or wireless router with an Ethernet connection. You also need a television source (antenna, cable, satellite, DVR, DVD, or video camera), a high-speed Internet connection (for remote use), and a PC with Windows 2000/XP.

You should know that, although the Slingbox is a networked device, only one person can use a Slingbox to view television at any one time. For simultaneous viewing, you need multiple Slingboxes.

For a wired connection, attach the Slingbox to the router with the included Ethernet cable. However, because the device must also connect to the video source and your router may be elsewhere in the house, the manufacturer offers SlingLink Powerline wall plug Ethernet adapters (two for $99; www.slingmedia.com). The SlingLink bridges use existing electrical outlets and wiring to connect the router's Ethernet signal to the Slingbox. An Ethernet cable runs from the Slingbox (which is connected to your TV) to one wall plug bridge, and another Ethernet cable runs from the router to a second wall plug bridge. (Note that older homes without modern wiring may not support the wall plug bridge solution.)

If you have a wireless network, the Slingbox cannot connect to it directly. However, you can purchase an Ethernet-to-wireless bridge device, such as a wireless game adapter, to do the job. Be sure to purchase a wireless bridge that's compatible with your wireless router/AP (such as 802.11b or 802.11g) and that supports the level of security you want to use (WEP, WPA, WPA2). Follow the bridge manufacturer's instructions for setup and configuration, and connect it to the Slingbox with an Ethernet cable.

The Xbox 360 has its own wireless adapter that snaps into place on the game controller.

D-Link MediaLounge DSM-520. The D-Link MediaLounge DSM-520 ($249; www.dlink.com) is a comprehensive multimedia hub, a wireless media player that connects your networked computers' digital audio, video, and photos to your home entertainment system. In addition to most standard PC multimedia files, it supports streaming of HD video and photos, plays DRM-protected music files from Napster and Musicmatch, supports a variety of AOL services, and handles Rhapsody's audio-streaming service. What's more, portable devices (but not iPods) can connect to the DSM-520's front USB drive to play multimedia files through a home entertainment system.

To use the DSM-520, you need a television or other video device to display video and the media player's menus, an audio output device, one or more Win2000/XP PCs, and a home network with an 802.11b or 802.11g wireless router or a wired Ethernet router. After you connect the video, audio, and network devices to the media player, you use the on-screen instructions to configure the network connection and other settings.

When you set up the DSM-520 on a wireless network, the system asks for the SSID, level of encryption security (the DSM-520 supports WEP and WPA), the encryption key passphrase, and other information. If your PC runs WinXP with SP2 (Service Pack 2), you can simplify the wireless setup with Windows Connect Now and a USB flash drive. To access Windows Connect Now on a PC that already has a wireless connection, click Start, All Programs, Accessories, Communications, and Wireless Network Setup Wizard. Follow the on-screen instructions to add a new device to your wireless network (the DSM-520) and copy the wireless network configuration information to the USB flash drive.

When your DSM-520 is up and running, you can install the companion D-Link Media Server software on each PC that you want to pull multimedia files from. After configuring the software, the DSM-520 lets you access multimedia files from any of the Media Server PCs and play them on your home entertainment system.

Microsoft Xbox 360. Microsoft's newest game console offers users more than just games. It also plays music from connected MP3 players (including iPods), displays pictures stored on your digital camera, and shares media files from a WinXP SP2 or WinXP Media Center PC. To play music and display pictures from portable devices, you simply connect a player or camera to the Xbox 360's USB port. To share media files, you need to connect the Xbox 360 to your home network.

With an Xbox 360 connected to your network, WinXP SP2 systems

Quick Links | Home | Worldwide
Windows Media
Search Microsoft.com for:
Go
Windows Media Home
Windows Media Worldwide
For Home
Windows Media Player 11
Windows Media Player 10
FAQ
Extras
Previous Versions
For Windows Mobile
For Mac
Music & Video
Cool Devices
For Professionals
Enterprise & A/V Pros
Resources
Downloads
Support
Community
Windows
Media Connect 2.0
With Windows Media Connect, you can use a digital media receiver (DMR) to experience music, photos, and movies stored on your Windows XP–based computer anywhere in your home.
MORE WAYS TO ENJOY MUSIC AND VIDEO
Bring the entertainment you have stored on your computer to every room in your home:
Play Music
Listen to music on your home stereo system from your computer.
XBOX 360
Xbox 360 meets the Player
Stream music and photos from your Player library to your living room with Xbox 360

Windows Media Connect software delivers music, photos, and videos from WinXP PCs to multimedia devices, such as a TV or audio player.

can share photo files and unprotected music files, and you can play the files from your PC on your home entertainment system. If you connect an Xbox 360 to a WinXP Media Center PC, you can use the 360 to record shows, watch video, and watch, pause, and replay live television.

The same connections that let you access Xbox Live (the Xbox Internet-based gaming service) also support media file sharing. For a wired connection, you need an Ethernet cable and a router that's compatible with Xbox Live (see www.xbox.com/en-US/support/connecttolive/xbox360/homenetworking/equipment.htm). Simply connect an Ethernet cable to the Ethernet port on the Xbox 360 and to an Ethernet port on the router.

To connect the Xbox 360 to your home network with a wireless connection, purchase the Xbox 360 Wireless Adapter ($99.99; www.xbox.com). The adapter is compatible with 802.11a/b/g wireless networks, and it supports WEP and WPA encryption. After you attach the wireless adapter to the Xbox 360, go to www.xbox.com/en-US/support/connecttolive/xbox360/connectionmethods/webconnectivitywizard.htm and run the wizard for step-by-step Xbox setup instructions customized for your ISP (Internet service provider) and system configuration.

After connecting the Xbox 360 to your home network, you can configure a PC running WinXP SP2 or WinXP Media Center to share media files. To do this, log on to www.xbox.com/pcsetup from the WinXP SP2 or Media Center computer. This displays the Xbox 360 Media Setup interface. Follow the on-screen prompts to configure media file sharing.

Share Music

If your goal is to share music files from an iPod, MP3 player, or a networked computer, there are a number of devices to help you accomplish this. As of press time, we did not find a portable MP3 player with built-in Wi-Fi or Ethernet connectivity. However, some docking stations and specialty devices offer easy ways to share music files around the house.

iPod. If you have a network, you can share iTunes music among your PCs. The software supports sharing a single computer's library with all other computers on a network, and sharing separate libraries on multiple computers across the network.

If you want to take multimedia sharing to the next level, consider a dock that turns the iPod into a multimedia hub. A good example is the Griffin TuneCenter ($149.99; www.griffintechnology.com). The TuneCenter works with older iPods, including third-generation versions and the iPod mini, the newer iPod nano, and iPod with video. It can connect to your home network with its built-in Ethernet port or wireless 802.11b connection and play Internet radio on your home entertainment system. The device also connects your iPod to your television for on-screen menus, digital photo display, and iPod video viewing.

Music anywhere. If you'd like to listen to your PC music library as you're drifting off to sleep, a network-aware music player could be the ticket. Products such as the Roku M1000 SoundBridge Network Music Player ($199.99; www.rokulabs.com) connect to your home network and play digital music from your computer. The M1000 supports networking via wired Ethernet and wireless 802.11b with WEP encryption. It has built-in support for most music player software, including iTunes, Windows Media Player 10, and Rhapsody. You can connect stereo speakers or powered speakers to the device, and it also plays Internet radio stations.

The Slim Devices Squeezebox ($249.99 wired only, $299.99 wired/wireless; www.slimdevices.com) is a similar product that finds music files located on your home network and plays them wherever you locate the device. The pricier version includes both 802.11g wireless (with WEP, WPA, or WPA2 encryption) and Ethernet connectivity, and it can work as a wireless bridge for additional Ethernet-ready devices. It comes with its own SlimServer software for locating and managing music files on your network.

The wired and wireless home is no longer a thing of the future. Today, you can link your home network, entertainment system, and multimedia devices. If you're wondering what to do next with your home network, try connecting a multimedia device and take your home network to the next level. RS

BY CARMEN CARMACK

Gaming Goes Online

Connect Your Console To The Internet

In the "Good Ol' Days," if you wanted to play Pong against your cousin who lived across the country, driving there was the only way to do it.

But video games have grown up alongside the Internet. Although you could play video games online with a PC or Mac long before major console makers such as Sony and Nintendo built systems that could access the Internet, today it's easy to connect a video game console to the Internet. Portable video game systems give you the opportunity to compete against friends over a WLAN (Wireless Local-Area Network) or surf the Internet with a built-in Web browser.

Whether you're a gamer seeking to connect your system for the first time or seeking to earn the Grandparent of the Year award when your grandchildren visit you for Thanksgiving, we'll show you how to configure and connect three consoles (PlayStation 2, Xbox, and Xbox 360) and two handhelds (PlayStation Portable and Nintendo DS) for online access.

Connect Your Consoles

The PS2 and Xbox were the first systems from Sony and Microsoft, respectively, to connect to the Internet, but that's about where the similarities end. Microsoft included a built-in Ethernet adapter and developed the Xbox Live service, which is similar to Grand Central Terminal for Xbox gamers; Sony's first PS2 models required an aftermarket adapter that could connect via a broadband or dial-up Internet connection and didn't offer a centralized gaming service for gamers. Sony later introduced a slimline PS2 that included a built-in Ethernet adapter, but the console still lacked a centralized service. The Xbox 360 also includes a built-in Ethernet adapter and uses Xbox Live.

Under the assumption that most people would not want to use their broadband Internet access solely for online gaming, we used a Linksys WRT54GS wireless router to share Internet access among our PC and game consoles.

PlayStation 2. To connect an original PS2 to the Internet, we purchased the Network Adaptor (sic). We located the expansion bay cover on the back of the PS2 and pried it off with a flathead screwdriver. After unplugging our PS2 and lining up the adapter's male connector with the PS2's female expansion port, we pressed the adapter firmly in place and secured it by tightening the adapter's screws. Next, we linked the PS2 to one of our router's open LAN ports with an Ethernet cable.

Once we connected our hardware, we turned on the PS2 and inserted the Network Adaptor Startup Disc, which came with the network adapter. (*Note: Sony has released different versions of this disc, so configuring your console may involve slightly different steps.*) We used our controller's D-pad (directional pad) to select ISP Setup. We pressed the X button to continue. The configuration software displayed a loading screen. We pressed X after seeing the following on-screen message: Welcome To Network Adaptor Start-up Disc.

At this point we inserted a PS2 memory card in the appropriate slot on the console because PS2 needed to save network settings. We pressed X and skipped registration on the next

screen by pressing the square button. We pressed X to advance the next three screens. Next, we had the opportunity to name our connection. We used the D-pad to highlight letters on the on-screen keyboard and pressed X to select them. When we finished choosing a name, we highlighted Enter and pressed X.

The configuration software then asked if we subscribed to an ISP. We highlighted Yes and pressed X. On the next screen, we highlighted High Speed Connection (Cable or DSL) and pressed X. We selected Automatic Settings and pressed X. When asked if our ISP required a user ID and password, we selected No and pressed X. If your ISP does require these, choose Yes and enter them with the on-screen keyboard you used to name the connection.

The software asked if our ISP required a DHCP (Dynamic Host Configuration Protocol) host name; we selected No and pressed X. Although most broadband connections don't require a DHCP host name, follow the same general steps as entering an ISP user ID and password if your connection requires one. You can contact your ISP to determine if you need to enter a DHCP host name.

Once you complete these steps, the Network Adaptor Startup software will test your network connection. It gave us a Congratulations! message stating that our PS2 was network-ready.

When you want to play PS2 games online, be aware that each game may have a different method of accessing online content. Usually a game's main menu will have a multiplayer option that lets you access its online material.

Xbox. Although the Xbox and Xbox 360 have the benefit of Xbox Live, the gateway to playing Xbox titles online against other gamers, the service isn't free. You can purchase a 12-month subscription card, three-month starter kit, or 12-month starter kit for $49.99, $39.99, and $69.99, respectively. Both starter kits include an Xbox Communicator headset, and the 12-month kit includes a copy of Project Gotham Racing 2. The three-month kit contains a demo disc with two games. Two-month subscription cards are available in many games, and you can continue your subscription with a credit card or additional subscription cards.

Using an Xbox with an existing Xbox Live account, we connected our Xbox to our router like we connected the PS2. We started the console and used our Xbox controller's D-pad to highlight Main Menu. We pressed the A button to continue. Next, we selected Network Settings and pressed A. Finally, we highlighted Connect and pressed A. The Xbox automatically went through the following steps: checking for cables, configuring IP settings, resolving the DNS (Domain Name System), and connecting to Xbox Live.

On our first attempt, the connection utility notified us that it couldn't connect to Xbox Live. Upgrading our router's firmware solved the problem (you may not have to upgrade your router's firmware to use Xbox Live, but follow your router's manual for directions if you're having similar trouble initially connecting). We retested the connection after completing the firmware upgrade and received a Connected To Xbox Live message. We highlighted Done and pressed A. We pressed B twice to return to the Main Menu.

We used the D-pad to highlight Xbox Live and pressed A. Next, we selected our account and signed in by pressing A. When you start an Xbox game with online play, you may have to sign in again.

Xbox 360. With a properly configured and current Xbox Live account, connecting an Xbox 360 to the Internet and signing into Xbox Live is a cinch. We attached an Ethernet cable to the Xbox 360's Ethernet adapter and an open LAN port on our router. After we turned on the console, it automatically detected our profile and signed us in to Xbox Live. To confirm this, we went to the Xbox Live tab and noted that Xbox Live had signed in our profile (see photo). Unlike the original Xbox, we didn't need to update our router's firmware for the Xbox 360 to connect.

Before Sony introduced its remodeled PS2, you had to attach an aftermarket network adapter to its expansion port if you wanted to connect the console to a network.

You can still test your connection manually. We used the D-pad to switch to the System tab and highlighted Network Settings. We used the D-pad to highlight Test Xbox Live Connection and pressed A. The Xbox 360 will test for connectivity and notify you if it passes each test.

The Dashboard's Xbox Live tab has plenty of online content that goes beyond merely battling it out online in a particular game. You can download

movie trailers, game demos, or access the Xbox Live arcade.

If you already have an Xbox Live account from the original Xbox, you can migrate your account to an Xbox 360 during the initial setup. At the Gamer Profile screen of the initial setup, use the D-pad to select I Am A Member Of Xbox Live and press A. Follow the on-screen instructions to complete the transition.

A Portable Portal To The Web

Imagine yourself sipping a Venti latte in a Starbucks when the friend you're waiting to meet calls you with news that she'll be delayed an hour. The PSP (PlayStation Portable) and Nintendo DS are equipped with built-in wireless adapters, letting you connect at hotspots around the world or, with a wireless router, within the comfort of your living room.

PlayStation Portable. Although Sony may have dragged its feet in integrating a network adapter into the PS2, it wasted no time giving the PSP an 802.11b wireless adapter from the beginning. And, as a bonus, the PSP's Firmware 2.0 includes a Web browser, letting you surf the Internet when you're not gaming.

Before turning on our PSP, we flipped the wireless adapter's on/off switch (in the lower-left corner of the device) to the on position by sliding it up. Next, we turned on the PSP. On the main menu, we pressed the left D-pad button to select Settings and pressed the down D-pad button to Network Settings. We pressed X to set up our wireless connection.

We used the D-pad to select Infrastructure Mode (use Ad-hoc mode to establish a connection between two PSPs without a wireless router) and pressed X. The PSP displayed a Create A Connection message, and we pressed X to advance. Next we named our connection. You can create a number of connection profiles. The PSP labels the connection "Connection 1" by default. If you want to rename this, you can shift to a screen that lets you name the connection profile. We left the profile with its "Connection 1" name and pressed the right D-pad button (*Note: "right" in the PSP tutorial refers to the PSP's directional button; in this context, "right" does not mean "correct"*) to advance to the next step.

On the next screen, the PSP gives you the option of scanning for all available SSIDs (Service Set Identifier, or a wireless network's name) or manually entering a specific SSID. Automatic should be selected by default; we pressed the right D-pad button to let the PSP scan for available SSIDs. Once it finds your SSID, it should identify what method of wireless encryption, if any, your wireless network uses. If your network does have wireless security (we recommend it does), the PSP (with Firmware 2.0) supports the following encryption standards: WEP, WPA-PSK (TKIP), and WPA (AES). We had our wireless network set up with WEP encryption, so we made sure we highlighted WEP and pressed X. We entered our network's WEP key on the next screen, and when we finished, we highlighted Enter and pressed X.

After we entered our WEP key, we pressed the right D-pad button. For Address Settings, we highlighted Easy (the PSP should highlight it by default) and pressed the right D-pad button. We reviewed our settings, pressed the right D-pad button and X to save our settings. Finally, we pressed X, and the PSP tested the connection. After the test was successful, we pressed the circle button to quit the setup.

Once you setup an Infrastructure connection, you can use PSP's Web browser or play online multiplayer games against your closest friends or complete strangers.

Nintendo DS. Like the PSP, the Nintendo DS lets you play against others over an Ad hoc or Wi-Fi (802.11b) network, but it didn't include a Web browser at press time.

The Nintendo DS offers two flavors of wireless play: over the Internet and in Ad-hoc mode. To play online, you'll need a game compatible with Nintendo's WFC (Wi-Fi Connection). And if you don't have access to a hotspot, the Nintendo DS also requires a broadband Internet connection and wireless router. Starting a multiplayer game in Ad-hoc mode simply requires another Nintendo DS; the two handhelds can communicate wirelessly.

We inserted a Mario Kart DS, a Nintendo WFC-compatible game, into the Nintendo DS and turned it on. After the Nintendo DS started, we touched its touchscreen with the stylus and touched Mario Kart DS. At the Mario Kart DS start screen, we touched Nintendo WFC. Next, we touched Nintendo WFC Setting, Nintendo Wi-Fi Connection Settings, and Connection 1. Although the Nintendo DS automatically detected our wireless router, you also have the option of manually entering your SSID (Service Set Identifier). It prompted us to enter our WEP key, which we entered by touching the corresponding keys on the touchscreen and touched OK to enter. We touched OK to test the connection, and the Nintendo DS confirmed we had a successful connection.

With the connection selected, we touched Back twice and Nintendo WFC Match. Next, we touched Yes and selected the location of our opponents (you can choose from Friends, Regional, Worldwide, and Rivals).

A World Of Opponents At Your Fingertips

If you crave those "Good Ol' Days" of actually seeing your opponent, there's nothing wrong with connecting an extra controller, pulling up another recliner, and playing head-to-head (or cooperatively). But today's consoles that connect to the Internet for multiplayer excitement are simply opening up new realms of possibilities. It's your decision to explore them. RS

BY VINCE COGLEY

Home Automation Setups

Make Your PC Your Security Guard

There are three major reasons to invest time and money in a home automation setup. The first is convenience; the second is security and safety; the third is energy savings. Convenience is the hardest sell, but when you consider that many technologies are essentially things of convenience, it's easy to understand. Security and safety sell much better. On the security front, homes get broken into when they're empty, and they can get vandalized whether we're in them or not. Nurseries need monitoring, as well. Home automation systems let you monitor any part of your house, inside or outside, wherever you place your cameras. As for energy savings, these systems can certainly help. You can divide your house into zones and have them heated individually and appropriately, for instance. But every time you add sensors and controllers, the cost of your entire system goes up, so energy savings do not necessarily translate into cost savings.

To automate, control, and monitor your home, you need a variety of product types, ranging from programmable electrical modules to security cameras and specially designed switches. You need one or more types of hardware equipped with protocols for controlling the devices, and you need software for your PC to combine the items into a manageable system. If you want to work with your devices on your home network, you need a wired or wireless network in place so that the devices can become nodes on that network. And if you want to take the next step, controlling and monitoring your devices over the Internet, you need an Internet connection (ideally an always-on broadband connection) and software that can control the items, serve the images, and (if you want live viewing) stream the video.

Fortunately, such products are becoming increasingly easy to get. Software packages such as PowerHome ($69.95; www.myx10.com), HomeSeer HS2 ($199.95; www.homeseer.com), and Girder 4.0 Standard ($49.99; www.promixis.com) let you control a variety of devices. Here, we look at three common and easily managed setups, designed to get you started with what can easily become a fascinating and absorbing long-term project.

Set Up A Security Web Cam

The easiest way to start monitoring your house is by purchasing a kit designed specifically for this purpose. Motorola offers its homesight Wireless Easy Start Kit ($299.99; broadband.motorola.com/consumers/products/hmez2000), which contains a wireless camera, a wireless door/window sensor, a wireless system controller, and software to set up, configure, and monitor the system. We'll start with this product because it provides a good overview of how such systems work, although certainly you can do all of this without buying a dedicated kit.

First, install the software, which you will use to detect the devices and control them. The next step is to install the hardware. The wireless system controller plugs into your PC's

USB port, and if you intend to do remote monitoring, your PC must in turn be connected to the Internet through a broadband connection. Next, place the wireless camera in the room you want monitored, mounting it on a table, the floor, or (by using the included brackets) on the wall, and then aiming it so that you can see the area that you wish to monitor. Next, install the wireless door/window sensor, which you attach to the door or the window you wish to monitor. The sensor is in two parts: one attached to the frame, the other to the window or door. The idea is that the two parts provide a connection, and as long as the connection is intact, the software does nothing. When the window or door is opened, the connection is broken, and a signal alerts the software, which in turn alerts you.

Once you have the hardware set up, you use the software to monitor it directly—in the case of the camera—and to tell the hardware how to respond to various events. This is the programming aspect of home control software, and while it sounds somewhat difficult, the software packages step you through the process via a combination of wizards and selection menus. For example, you can tell the Motorola software to send an audio alert whenever the connection on the door/window sensor is broken. You would use this either to detect an intruder or, more commonly, to tell you that someone you've been expecting (such as your child) has arrived. However, you could also set the camera in place to view the doorway, and then configure the software to alert you when the sensor's connection is broken when the door opens *and* to turn on the camera and provide either still pictures or video that you can view on your PC.

Motorola's kit can notify you of events in three ways. First, if you're in the house, it can flash alerts on your PC. Second, it can email alert messages, pictures, and video files to you. To have it do so, you need to configure the control software with your email information (including the outgoing mail server details). Third, you can configure it to send alert messages to your cell phone and, if your phone is capable of displaying images and even video, it can send graphics and video files along with the messages. Once again, you need to configure the software with your cell number, specifying which events you want to be alerted about and what information you want sent to you this way. You can set up multiple cell phones, in fact, with each one receiving different (or the same) information.

You can remotely monitor any room in your home with a security camera such as this one from Linksys.

Obviously, to monitor, control, and automate your entire house, you'll need more hardware than you get with the Start Kit. For this purpose, Motorola offers wired cameras, day/night cameras, a wireless siren, and wireless water sensors, temperature sensors, and motion sensors.

You can get all of these things from other vendors as well, across today's full range of wireless and home control technologies. All you need, in addition to your home network and PC, are a Web cam and its configuration software, and either the Web cam's included viewing software or a Web browser. For this step-through, we'll assume that you want a wireless Web cam (in order to minimize wires and connectors) that you can view both locally and over the Internet.

Two recommended cameras are the D-Link DCS-G900 Wireless G Internet Camera ($151.99; www.dlink.com) and the Linksys WVC54G Wireless G Internet Camera ($109.99; www.linksys.com). Both connect easily to an existing 802.11g wireless network (both companies also offer 802.11b versions of the products), and both come with the software you need to configure the camera for capturing images or video under specific conditions and for remote viewing over the Web. Here we use the Linksys product as an example.

The first step is to add the camera to your home network. Place it near your wireless router/access point and run an Ethernet cable from an empty port on your router to the Ethernet port on the back of the camera's base. You can also configure it wirelessly, but to do so you need to temporarily reconfigure the access point to match the built-in settings on the camera, so that your access point can see it.

Now, connect the camera's power adapter, plug it into a wall socket, and turn on the camera and let your network find it. Install the software from the CD included with the package and step through the setup wizard. The wizard lets you set a username and password required for access to the camera, and it also provides the setup dialogs needed to establish the camera as a node on your wireless network. After you've completed this step, unplug the Ethernet cable to let your access point find the camera and include it on your network. Linksys provides a detailed guide on how to work with your access point to ensure that you've made the connection.

The next step is to install the Viewer and Recorder program on one (or all) of the PCs on your network. Here, you establish how to access the camera and the quality of the pictures or video you want to capture. The higher the quality, the better the image and video, but the greater the disk space used and the upload time to the Internet. You can also schedule recordings at specific times, and you can establish how long an unscheduled recording, such as an intrusion detection, is to last. Also from here, you can enable the camera to start capturing images or video automatically when motion is detected within a specified range. With these configurations in place, you use the Viewer to watch your camera in action.

Finally, install and configure the Web viewer, a separate item of software. If you have access to an FTP (File Transfer Protocol) server, you can have the software upload the images/videos there, so that you can view them on your browser that way. Alternatively, Linksys hosts the SoloLink DDNS Service, which dispenses with the configuration and security problems often encountered with viewing Web cams over the Internet by uploading the image and video files to that service and letting you view them on the service Web site. The service, which is highly recommended for reliable and secure viewing, is free for 90 days and then costs $20 per year.

Set Up A Wireless Media Player

Another product type with numerous variations today is the wireless media player, designed to stream audio and video from your networked PCs to your television, audio system, or other PCs. Media players are available from companies such as Hauppage (www.hauppage.com), whose Wireless MediaMVP sells for $149, and NETGEAR (www.netgear.com), who offers the Wireless Digital Music Player MP101, which of course streams audio only, for $89.95. Numerous products offer wireless streaming of iPods and other portable audio players.

The D-Link DSM-320RD Wireless Media Player lets you stream digital audio and video to your home entertainment center.

Here, we focus on both audio and video, and as our sample product we've chosen the D-Link DSM-320RD Wireless Media Player with DVD and Card Reader ($284.99; www.dlink.com). While certainly more expensive than some, it has the benefit of being able to stream not only files on your PCs, but also DVD video and images stored on a variety of memory card types. In other words, it's highly versatile, and can function as the centerpiece of your entertainment network.

The DSM-3200RD ships with an Ethernet cable, an S-Video cable, RCA cables, an antenna, software, and a remote control. You begin by installing the software and, during this process, specifying which media files/folders on your PCs you want to make available for sharing over the network. You also specify how often you want the software to scan the shared folders for new content—every half-hour, every hour, once a day, etc. You can use either the software included with the package or Windows Media Connect, available from the Windows Update site to anyone with Windows XP Service Pack 2. You can use both, in fact, which we recommend for maximum flexibility.

It's now time to connect the Wireless Media Player to your TV and audio systems. Place the unit near your entertainment center and run the cables from the back of the Media Player to your equipment. The unit provides three types of video connectors: composite video (RCA), S-Video, and component video. For sound and music, you can choose from standard RCA, optical digital audio, and coax digital audio connections. You need to supply your own cables if you want component video or either of the latter two audio connections.

Next, turn your TV on, select the input to which you've attached your video cables, and use the setup utility. Using the included remote control and the on-screen keyboard, start the Setup wizard. Your first choice is to select the network type. If you've plugged an Ethernet cable into the unit, choose Wired; if you plan to stream through your wireless network, choose Wireless. Assuming a wireless connection, from this point on you need to select or input the options needed to make the connection with your access point, although the Media Player will likely detect your network and either make the connection or start the process (letting you configure the specifics).

With the Media Player fully connected, the fun part begins. You can now browse for music or videos,

create playlists, view pictures and build photo albums, and watch DVDs. Any DVD or memory card inserted into the Media Player is available to you, as are online services such as RadioAOL and Live365 (and others) if you have accounts with those services.

Control Your Lights & Thermostat

By far the easiest way to start controlling and automating lights, thermostats, and other household items is by purchasing a starter kit. The granddaddy of such kit producers is X10 (www.x10.com), which offers a wide selection of bundles at prices ranging from $79.99 for The Complete ActiveHome Suite (seven items) through $219 for The Complete Active-Home Suite Plus Wireless Video Sur-veillance (18 items). Each kit includes software and a variety of hardware devices, ranging from standard modules for controlling lamps and other electrical appliances to cameras, capture modules, USB connectors, and more. Another company offering a range of kits is HomeSeer, whose Z-Wave PC Starter Kit sells for $126.95 and includes four items. The major difference here is the protocol: X10 uses the most well-established home control protocol of all, X10 itself (the company is named after the protocol), while HomeSeer uses the newer but more versatile and more reliable Z-Wave.

No matter which of these kits you choose, you'll find an endless array of add-on products to complement your system once you get it established. Examples include lamp modules, appliance modules, motion sensors, dimmer switch controllers, tabletop remote controls, car remotes, and thermostats, each of which costs between $37.95 to $269.05 for the Z-Wave versions and typically less for the X10 products.

For our sample here, we wavered between SmartHome's Ultimate Lighting Control Starter Kit ($188.99; www.smarthome.com) and the HomeSeer kit outlined above. Ultimately, we chose The Complete ActiveHome Suite from the X10 site because of its extensive array of devices and its relative lack of expense, the latter is especially true given the inclusion of control software. One reason to consider SmartHome, indeed, is its support for the INSTEON interface, which offers greater signal reliability than the X10 protocol but still retains full compatibility with X10. Z-Wave, by comparison, is not compatible with X10, which means that if you want to run X10 products through HomeSeer's software, you'll need a separate USB adapter ($39.95).

A home starter kit is the easiest way to automate your home.

The ActiveHome kit ships with four modules and three software packages. Installation is simple: You merely plug each module into a wall socket and then plug an electrical device (lamp or other appliance) into the receptacle on the module. You then install the included MyHouse Online software on your PC, load the program, and monitor and configure your modules. The most common scenario for a simple setup such as this one is to schedule your lights and other appliances to turn on and off at specified times. That's not much, but it's a start.

The next step is to add to your system once you get used to what it can do. The enormous variety of X10-compatible products makes the possibilities nearly endless. For example, the X10 Thermostat Setback Control ($19.95) plugs into an appliance module and mounts under your wall thermostat; it casts heat towards the thermostat, causing the thermostat to shut off the furnace. X10's software controls when the device turns on and off, allowing a simple but effective furnace control. X10 also sells dimmer switches, wireless cameras, and even a kit that makes barking dog sounds, all of them controllable via the software.

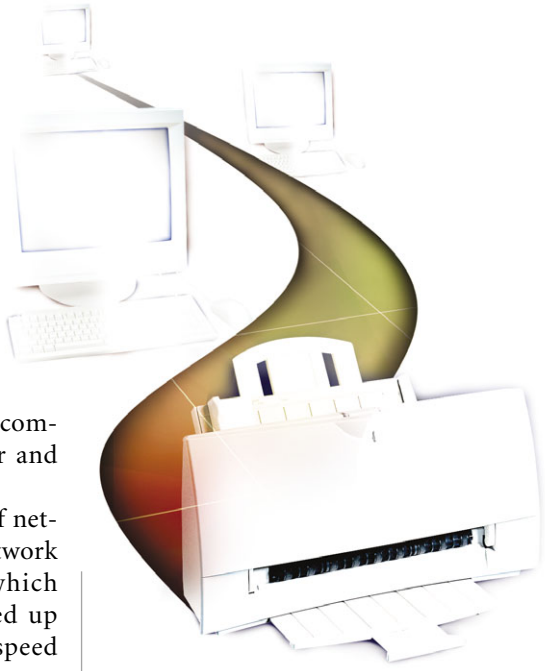
However, eventually you'll want to move into products with more professional capabilities, and here's where INSTEON and Z-Wave come in. HomeSeer's Z-Wave Communicating Thermostat, for example ($149.95), replaces your current thermostat and provides pinpoint control over your furnace and air conditioner alike. To use Z-Wave equipment, however, you will need compatible software, which means either buying the HomeSeer package itself ($199.95) or a third-party package such as Promixis' Girder Pro software package ($99.95). Girder Pro allows you not only full local control of X10, Z-Wave, and INSTEON equipment, but also provides control via the Internet.

The options for home control, automation, and monitoring are extensive and nearly unlimited. So, potentially, are the costs. For lighting and appliance control, buy a Starter Kit and see if you like the entire idea. For entertainment streaming, decide what your needs are and go with a media player that will fulfill *all* of them, not just one or two. For security and safety, start small—perhaps only one Web cam or one motion sensor—and determine what you need as you go along. As long as your purchases are geared toward expandability, you won't go wrong. RS

BY NEIL RANDALL

Print Connections

How To Install A Networked Printer



Back when Atari was on the bleeding edge of computing, pundits and so-called experts said that printers, printing, and paper would soon be a thing of the past. But they had no inkling of how cool today's printers can be. With fast output and snazzy color, printers from HP, Canon, Epson, and other manufacturers have impressive features, the type you may want to share by networking your printer.

But networking a printer can be daunting. There are so many options, and the instructions that came in the box can seem like they were written in Farsi, then translated to Dutch and Urdu before they made it to English.

Not to worry. We will take you through the process of setting up a printer on a network, and we'll give you all the background knowledge on networks and networking you need in clear and simple language. When you have the right information, networking a printer is not as hard as it seems. Just remember that the process may vary slightly from printer to printer and network to network.

Why Network?

First, a word or two on the benefits of networked printers. Of course, there's cost: You can share a networked printer with every computer on your home network, which means you don't have to buy a new printer for each computer (and empty your wallet in the process). It also means you can buy one really good printer with all the bells and whistles you want, rather than compromise on a bunch of smaller and less powerful printers.

What's more, certain types of network connections—built-in network adapters and print servers, which we'll explain below—can speed up your printing. These devices speed up the data transfer between your computer and the printer or print server; as a result, you can get on with your work more quickly. And having a single, shared printer means you'll have only one type of toner, ink cartridge, and other supplies to deal with. In our hyper-networked, information-anxious world, simplicity, like cleanliness, is certainly next to godliness.

Shared Printers

There are more than half a dozen ways to network your printer, but far and away the three most common—and most efficient—methods are using a shared printer, using a printer's built-in Ethernet adapter to attach it directly to your network, or using a small device called a print server.

Let's examine the first choice—using a shared printer—which is also the simplest. It takes no extra equipment; all you need is a single networked computer to host the printer (this computer is called the server, not to be confused with the print server explained below). Other computers will use the printer by sending a **print job** to the server, which in turn relays it to the printer. (A print job is simply a task you send to the printer, such as a graphic or spreadsheet to be printed.)

To get started, install your printer on the computer you plan to use as a server. Any computer will do, though you should choose one that sits in a convenient place. Just follow the instructions that came with your printer, which often go something like this: First, connect your printer to the server to trigger the Add Printer wizard. (If it doesn't appear, click Start, Printers And Faxes in Windows XP, or Start, Settings, Printers in Windows 2000, then click the Add New Printer button.) The wizard is easy to follow and walks you through your printer's setup, including the installation of printer drivers, which are small programs that let your computer talk to your printer and vice versa.

As an alternative to using the Add Printer wizard, your printer's user guide may instruct you to insert the CD-ROM that came with the printer, then take things from there. Either way, installing the printer on the server should be fairly painless and quick.

After you've installed the printer, it's time to share it. In WinXP, click Start, Control Panel, Printers And Hardware, then Printers And Faxes (or simply

Printers And Faxes if you don't see the Printers And Hardware option; depending on your Start menu's configuration, you may also be able to click Start, then Printers And Faxes); in Win2000, click Start, Settings, Printers. Locate the icon for the printer you just installed and right-click it, then choose Sharing from the context menu that appears. This will open the printer's Properties dialog box, which has several tabs across the top. By default, you'll be in the Sharing tab.

You may see a security warning at this point. Windows often does this because sharing your printers can open your network to attack if you're connected to the Internet and don't have a firewall, a device that filters your Internet traffic. If you'd like to continue with the printer installation, click the link to turn on printer sharing, then click the Share This Printer button.

When prompted, give your printer a name that tickles your fancy, such as Color Photo Printer, Living Room Printer, or even Matilda. Then click OK, and your printer is shared—that is, it's ready to be used by other computers on your network. Just go to those computers and launch the Add Printer wizard as explained above, then follow the prompts to install a network printer. You'll be asked to browse the network to locate the printer you just installed on the server. Once you have, follow the remaining prompts to finish the wizard. In a few minutes you'll have a fully shared printer on your network.

This quick and dirty way of sharing a printer is not without its drawbacks, of course. Chief among these is the fact that sharing a printer can disrupt printing for the person who's using the server, as all print jobs get routed through his or her machine. But the next method will take care of that problem completely.

Built-In Ethernet Adapters

A second way to network your printer is using its built-in Ethernet adapter, a device that lets you attach your printer directly to a network hub, router, or switch without using another computer as a server. Adapters, also called Ethernet cards, network cards, or even JetDirect cards (for HP printers), often come as standard features on business printers. If your printer doesn't have one, you can often buy one as an upgrade for $100 to $300. Network adapters used to be found almost exclusively on laser printers, but they're becoming more and more common on today's high-end inkjet printers, too.

Print servers, which let you attach a printer directly to your network without using another computer as a host machine, include an array of features. This model from NETGEAR has a single USB port for one printer.

To use your printer's Ethernet adapter, follow the instructions that came with the printer, which can vary from machine to machine. Often they'll prompt you to connect the printer, then insert the printer's CD-ROM into one of your network's computers. This will trigger the software to auto-run; it sets your printer's IP (Internet Protocol) address, the code that tells your network where your printer is located, and other network features as well.

Once it's done, you'll need to add the printer to each computer you plan to print from. To do so, go to one of your computers and click Start, Control Panel, Printers And Faxes (WinXP), or Start, Settings, Printers (Win2000). Then click the Add New Printer option to trigger the Add Printer wizard. This is where things can get a bit tricky. Why? Because you'll be asked to install a network printer or a local printer. Even though your printer is on a network, Windows views a printer that's directly attached to a network hub or router as a local printer. So choose that option, and deselect the Automatically Detect And Install My Plug And Play Printer option. Then click Next.

Now you'll select the Create A New Port option and choose Standard TCP/IP (Transmission Control Protocol/Internet Protocol) port. This will trigger a second wizard, the Add Standard TCP/IP Printer Port Wizard. (TCP/IP is a protocol that networked computers use to communicate.) In this wizard, you'll type the printer's name or IP address that you set up when you ran the printer's CD-ROM, then you'll click Finish to return to the Add Printer wizard, where you'll install the printer's drivers.

To do so, you'll be asked to choose your printer's make and model from an extensive list or to choose the Have Disk option, which tells Windows to search for the drivers on your printer's CD-ROM (an easier option). Once the drivers are installed, you'll be asked to name the printer (again, you can use any name you like), and follow the prompts to finish the wizard and exit. Your network printer will be installed and ready to use.

If this process seems daunting, remember that many printers with built-in Ethernet adapters have software that will take care of most if not all of this process for you. Just remember to consult your printer's user guide on each step, as the process varies from printer to printer.

Although setting up a printer with an Ethernet adapter is harder than a shared printer, it does have certain

Choosing A Print Server

Choosing a print server can be mind-boggling. There are so many to choose from, and their features vary widely, as does their cost.

First, of course, you'll need a print server that has the right connection type. Most use USB , but if your printer is an older machine with a parallel port, make sure your print server can accommodate it.

Next, you'll need to know how many printers you plan to use on a single print server. Do you plan to use just one, or do you intend to run two or even three printers off the same device? Print servers that accommodate more than one printer can be more expensive than basic models.

You'll also need to consider your printing volume. The cheapest, smallest print servers can handle most home or small office needs, but if you print a phone book's worth of documents each week, or if you have antsy users who don't like to wait for their print jobs to go through, you may want a print server that can deal with big jobs and heavy traffic. Check the vendor's Web site for stats on speed and volume, or read independent reviews that test different print servers for performance.

Last, of course, is price. You can buy a print server for as little as $50, and perhaps less if you're a price-shopping whiz. But print servers that can handle many printers and high volumes can run as much as $300. In the end, choose the one that suits your needs and won't break the bank. ❙

benefits. For instance, it connects your printer directly to your network, which means you don't have to worry about using another computer as a server. You can print more quickly, and you can even print if all the other computers on the network are turned off. But it's the next option—using a print server—that delivers the most bang for your networking buck.

Print Servers

A print server is a tiny box that connects your printer directly to a network hub, router, or switch, so you can share it among your network's computers. (Don't confuse it with the server mentioned above, which is a networked computer that's used to share a printer installed directly on it.)

Instead, think of a print server as an external Ethernet adapter. You plug your printer into the print server, and you plug your print server into a hub or router on your network. It also has some additional benefits over the built-in Ethernet adapter we discussed in the last section. First, a print server can have its own memory—sometimes lots of it—which transfers the burden of complex print jobs off of your computer and the printer itself and onto the print server, which can queue jobs. This makes all the difference if you print mountains of paper or frequently print very complex graphics, brochures, or posters.

A print server also gives you a single place to plug many printers into your network, even if they're different types of printers or have different types of cables (such as parallel and USB). And it lets you control print jobs from a central location, so you can cancel a job with ease or perform other printer management tasks. (Some print servers let you run diagnostics and use other features right through a Web browser on any computer on your network.) You can even use a wireless print server if your printer sits far away from a hub or router, and you don't want to run long, messy cables across your floor.

The bottom line? If you want to network your printer but don't want the problems of using a shared printer, or if your printer has no built-in Ethernet adapter, this is your best—and most powerful—option.

Setup varies from print server to print server, but it can be easy if you're using a newer print server and a recent version of Windows, such as WinXP or even Win2000. Most print servers come with built-in wizards to walk you through the setup. To start, you'll plug in the print server and connect it to a network hub or router (although with most print servers, you won't connect it to the printer just yet). Then you'll run the wizard by inserting the CD that came in the box, or typing a special address into a Web browser, such as Microsoft's Internet Explorer. You'll set the IP address and other network features using the instructions in your user guide, or the software will set them for you with little or no input. Often the whole process is largely automated.

During this process you'll also plug the printer into the print server and use the print server to set up the printer on your local machine (that is, the machine you're using). With some print servers, you'll simply install the printer using the normal Windows procedures, once your print server is installed and working. To do that, click Start, Control Panel, Printers And Faxes (WinXP) or Start, Settings, Printers (Win2000), then click the Add A New Printer icon to start the wizard. Follow the prompts to select a network printer and browse to locate the network printer on the print server. Then click Next and follow the prompts to completion, which takes under a minute.

That's not much time to invest in something as useful as a networked printer, which can save you not only time but also money on your day-to-day printing needs. And that will save you a few headaches, which may be the best payoff of all. RS

BY DAVID GARRETT

Share The Bandwidth

Set Up Internet Connection Sharing On Your PC

In today's world of endless connectivity and increasingly cheaper computers, it's not a stretch to see households using two or even three or more machines under one roof. Why constantly battle with Junior, who loves to play games and download music, when you can simply purchase an extra computer he can use and abuse to his heart's desire? More and more households are fully embracing this approach, much to the delight of PC and software manufacturers.

Unfortunately, multiple PCs must share a single connection to the Internet, usually a high-speed cable or DSL (Digital Subscriber Line) connection. To solve this problem and allow Junior to chat with his friends while you pay the bills online, you can set up a home network using a router and your existing cable or DSL modem. But, for many users setting up a home network can be a daunting task.

Enter ICS (Internet Connection Sharing), a Windows feature that lets multiple computers share an Internet connection by using one of the computers as a gateway. Read on to learn more about ICS, how to set it up, and how to troubleshoot and avoid possible pitfalls. You'll be sharing your Internet connection in no time.

ICS: Share The Pipeline

ICS first appeared on the scene with Windows 98 Second Edition and is a feature in every subsequent Windows version, including Windows 2000, Windows ME and Windows XP. As with most things Microsoft, the first iteration of ICS quickly developed a reputation as a balky, unreliable feature that could just as easily break your Internet connectivity as it could enable you to share it.

The main principle behind ICS is to enable sharing an Internet connection among several PCs through a single computer, called the gateway or the host. ICS can be used to share either a dial-up or high-speed connection, although it may not be very practical to share the already limited bandwidth of a dial-up connection, as each computer sharing the connection will only enjoy the use of part of the available bandwidth.

Another aspect of ICS is that it lets you share an Internet connection without needing a router to perform the various networking functions that connect your computers and printers to the network. If all your computers have NICs (network interface cards), you can connect them to each other using ICS. It's a way to enable networking without incurring the headaches that may come with setting up a network using a router.

ICS uses a service called **DHCP (Dynamic Host Control Protocol) Allocator** that performs the functions of a DHCP server that is usually part of most routers: it assigns IP (Internet Protocol) addresses to computers on the network and designates the network gateway (in this case, the host computer running ICS). ICS also features a **DNS (Domain Name Server) Proxy** (for translating network IP addresses into network names), **NAT** (Network Address Translation, for converting private network IP addresses into public addresses), and an auto-dialer for automatically dialing connections. Essentially, ICS converts the host computer into a networking

gateway by retrofitting it with the services needed to perform that function.

Host Preparation

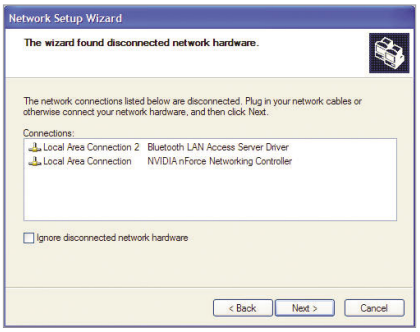
To set up a network using ICS, you must first install ICS on the computer in your network that is directly connected to the Internet via your cable or DSL modem; this computer will serve as the host/gateway. For ICS to work, this gateway computer must be running Win98SE or later. This restriction doesn't apply to the other computers in your network; ICS can connect all versions of Windows from Windows 95 on up.

If the host/gateway computer is connected to a high-speed DSL or cable connection, that computer must have *two* NICs installed to make ICS work. If the computer you intend to set up as the host doesn't have two NICs installed, the option to install ICS is not even available in Windows (at least not in WinXP). The idea is to connect one NIC to the cable or DSL modem while the other NIC connects to the other computers in your network. Also, it's important to recognize that ICS must be installed on the host computer that is connected to your cable or DSL modem.

After you designate your gateway/host computer, set up the cabling and any hardware you'll need to connect all the computers together. You'll need CAT5 cabling to connect all the computers to each other, and all computers must have NICs installed. A **hub**—a hardware device that serves as a common connection point for multiple computers—will make your life easier, especially if you're connecting more than two computers. Simply connect the CAT5 cabling from each computer's NIC into an open port on the hub. Then, connect the host/gateway computer to an available port on the hub.

Install ICS On The Host PC

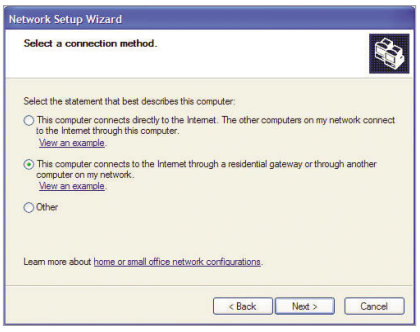
Once your cabling arrangements are in place, it's time to install ICS on


Network Setup Wizard
The wizard found disconnected network hardware.
The network connections listed below are disconnected. Plug in your network cables or otherwise connect your network hardware, and then click Next.
Connections:
Local Area Connection 2 Bluetooth LAN Access Server Driver
Local Area Connection NVIDIA nForce Networking Controller
Ignore disconnected network hardware
< Back
Next >
Cancel

The ICS (Internet Connection Sharing) wizard warns you if you have any disconnected Internet connections. You can also choose to ignore the disconnected connections by clicking the Ignore Disconnected Hardware checkbox.

the host computer. The easiest way to do this is to run the Network Setup Wizard. To access the Network Setup Wizard, click Start, then Control Panel. If you're in Control Panel's Category View (in WinXP), click the Set Up Or Change Your Home Or Small Office Network link to launch the wizard. Click Next until you see the Select A Connection Method window and be sure to choose the This Computer Connects Directly To The Internet option.

This option makes sense, because in ICS, the only computer with a direct connection to the Internet is the host/gateway computer. All other computers in your network connect to the host computer, through which they access the Internet and each other. So, when setting up ICS, the ". . . Connects Directly To The Internet" option is selected only once, for the host computer.


Network Setup Wizard
Select a connection method.
Select the statement that best describes this computer:
This computer connects directly to the Internet. The other computers on my network connect to the Internet through this computer.
View an example.
This computer connects to the Internet through a residential gateway or through another computer on my network.
View an example.
Other
Learn more about home or small office network configurations.
< Back
Next >
Cancel

It's very important to select the correct connection method when setting up ICS on the host computer.

The host computer is equipped with two NICs, one connecting it to the public Internet and the other connecting it to the other computers in your private network. Be sure to choose the connection that connects the host computer to the public Internet in the Select Your Internet Connection window. This step may seem obvious, but unfortunately, the wizard makes it a bit difficult to distinguish between the two adapters listed in the Select Your Internet Connection window. If need be, double-check this before proceeding, as making the wrong choice will force you to start all over again.

The next two steps in the wizard will ask you to assign the host computer a name and description and then assign a name to the network. For the computer name, select something that identifies the PC, such as "Office" or "Dad's PC"; also, use "host" somewhere in the computer description. That way, if you ever have to ascertain which computer is the host when troubleshooting, it will be easy to do so. For the network name, you can accept the default "MSHOME" network name and move on, but users often change it to something else, which we recommend.

On the final step, you will be asked if you want to finish the wizard or create a Network Setup Disk. If your client computers run WinXP or WinME, select the Just Finish The Wizard option (WinME has its own version of the Network Setup Wizard). If your client computers run any other version of Windows, choose the Create A Network Setup Disk option. This process copies a file called Netsetup.exe onto a floppy disk, which you can then use to set up your non-WinXP, non-WinME computers.

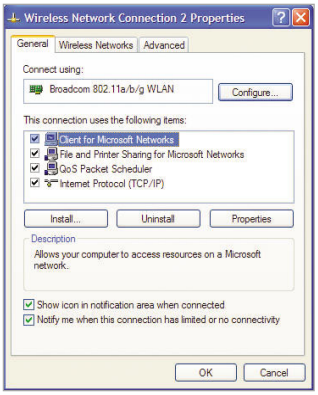
The Clients

Setting up the client PCs to work with ICS is actually quite simple, because the ICS service does not need to

be installed on the client computers. But, in order to get your other WinXP computers connected to your network, you must run the Network Setup Wizard on each one. Activate the Network Setup Wizard on each of the computers you want to connect by clicking Start, Control Panel, Network And Internet Connections, and clicking the Set Up Or Change Your Home Office Or Small Office Network link.

Follow the wizard, and be sure to choose the This Computer Connects To The Internet Through Another Computer On My Network option. Follow the remaining steps, and restart the computer if prompted to do so. Now, the client should be ready to connect to the Internet and your private network on the host computer. Do the same for all the computers you want to connect using ICS.

To set up any non-WinXP, non-WinME computers in your network, simply insert the disk you created into each client's floppy drive and run the Netsetup.exe file. When prompted, select the This Computer Connects To The Internet Through Another Computer option, give the computer a description and a name, complete the wizard and restart the computer when prompted.



The Network Connection Properties window is the place to verify that all the required clients and protocols are installed. In this example, it's easy to verify that the Internet Protocol (TCP/IP) is attached to the Broadcom 802.11 a/b/g WLAN (wireless local-area network) adapter.

Troubleshooting

As with anything else in Windows, there are times when things will go awry. Start by checking for the simple things first. Is your host computer's Internet connection working properly? If the Internet connection is not working, nothing else will. Are all cables securely connected and in the right places? A loose cable may be hard to find but easy to fix once it's found. Is a software firewall you recently installed not playing nice? Software firewalls, if improperly configured, can block the network traffic required for ICS to work properly. Consult your firewall documentation if you need help configuring your firewall. Also, for ICS to work, your host computer must be on and connected to the Internet.

You must ensure that a host/gateway computer equipped with two NICs has all the appropriate clients and protocols bound to *both* adapters. The Network Setup Wizard is a smart tool and will, in most cases, seamlessly install all the various protocols and items you'll need to make ICS work. But, things can and do go wrong from time to time.

To verify that all the required clients and protocols are installed on your host PC, click Start, Control Panel, click the Network And Internet Connections icon (if you're in WinXP's Control Panel Category view), and then click the Network Connections icon. Right-click one of the network connections displayed in the Network Connections window and click Properties.

The General tab in the Properties window shows you the hardware adapter (NIC) associated with this connection in the textbox titled Connect Using and also shows the various clients and protocols associated with this adapter in the This Connection Uses The Following Items list box. You should see, at least, Client for Microsoft Networks, File and Printer Sharing for Microsoft Networks, and Internet Protocol (TCP/IP) on the list. If one of these items is not present, click the Install button to add it. Follow these steps again for the other network connection in your host system. Finally, use these same steps on each client PC to make sure that each has all of these protocols installed.

Also, if you are sharing a dial-up connection, a dial-up adapter should be one of the items listed in the Properties window. And, if you are sharing a dial-up or ISDN (Integrated Services Digital Network) connection to access the Internet, be sure to choose the Establish A Dial-Up Connection Whenever A Computer On My Network Attempts To Access The Internet option in the wizard. Otherwise, a client computer attempting to access the Internet will not able to connect because the Internet connection it requires won't be available.

ICS: Old Technology?

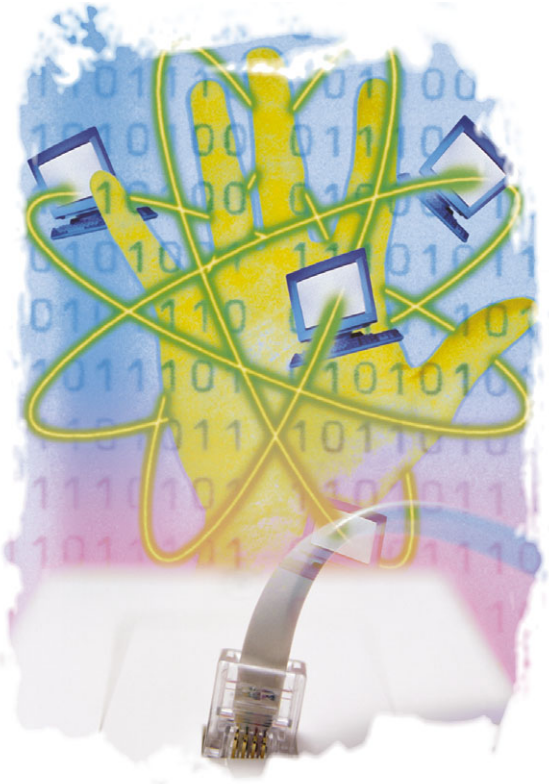
Today, consumers are using home networking to connect multiple computers and make the most out of a single Internet connection. It doesn't make any sense whatsoever to pay for multiple Internet connections when one will do, and ICS is an excellent option for connecting multiple computers together.

But, the easy availability of low-cost routers designed for home networking presents ICS with some significant competition. A hardware router provides many advantages over ICS, such as built-in DHCP, NAT, MAC (message authentication code) address filtering and various other features for configuring and customizing a home network. Still, these devices can present a significant learning curve to configure properly and can be challenging to troubleshoot if things go south. ICS is a good alternative if you choose not to use a router to set up your network. RS

BY SIXTO ORTIZ

How To Share Your DSL Connection

Advice For A Fast & Easy Setup



When you were a kid your parents told you to share and share alike. It was good advice, just as valid for a DSL (Digital Subscriber Line) Internet connection as for toys in the sandbox.

Sharing gives broadband speed to everyone on your home or small office network, meaning they'll get more done in less time. They'll also avoid the frustration of glacial downloads over plain old telephone lines. But before you get started, you'll need to know how sharing impacts your DSL. Simply put, it slows things down, but only when two or more users share the line at once.

Of course, if your DSL is fast enough to begin with, sharing may not make a dent in your downloads. To learn exactly how fast your connection is, just Google the term "bandwidth speed test" and use one of the free tools you find, such as the one at www.bandwidthplace.com/speedtest. It takes a few seconds to check your connection and tell you the true speed of your DSL. If it's above 1Mbps (megabit per second), sharing won't affect your speed for basic Web surfing.

There are dozens of ways to share your DSL, and your ISP (Internet service provider) may have special instructions, software, or even equipment to help you. If that's the case, follow your ISP's instructions carefully, and call its support line if you hit choppy waters. There are also a number of well-known methods that work for most networks, and we'll outline the two most common below.

The first (and far and away the simplest) is to use Windows' ICS (Internet Connection Sharing). It's quick and involves no extra equipment. The second way is more involved but has more benefits. It involves the use of a broadband router to link your network to the Internet.

Note that in the explanations below, we assume you've already installed a home or small office network and set up your DSL on at least one computer.

Get The Words Right

Before we get started, let's define some widely used terms related to DSL sharing.

First is **PPP**, or Point-to-Point Protocol. It's a **protocol** (that is, a way for computers to communicate) that's used to connect a single computer to the Internet. PPP is used on old analog modems, the type that few people use these days. More common is **PPPoE**, or Point-To-Point Protocol over Ethernet, which is designed to connect the many computers in a home or small office Ethernet network to the Internet. Ethernet is a type of network that was first designed by Xerox in the late '70s, and it's far and away the most common type of network in SOHO—small or home office—applications. It runs at 10Mbps. You may also have heard of Fast Ethernet, which runs at speeds up to 100Mbps. Some Ethernet gear can even run at 1,000Mbps, or 1Gbps (gigabit per second). You will run into these terms if you use the instructions or equipment that came from your ISP.

Because you've already set up your home or small office network, you've also seen terms such as hub, switch, and router, but we'll review them again, given their importance. A **hub** is a small device that connects more than one computer together. It's about the size of two decks of cards, and it's one of the simplest tools you can use to string your computers together into a network.

A step up from a hub is a **switch**, which you can think of as a smarter version of a hub. Unlike a hub, a switch carefully routes network traffic that goes through it, so that

data moves through your network more efficiently.

A **router** is more complex than a hub or a switch, and it's used to connect two networks to each other, such as your home or small office network to the Internet. Routers have all the traffic routing features of a switch, plus a number of security functions that protect your network. For instance, routers use a technology called NAT, or Network Address Translation, to hide the network address of the computers that use the router. This means that only your router can be seen by users outside your network, which protects the computers inside your network from hackers.

Some of today's routers—especially the kind you buy in your local computer store for the express purpose of home or small office networking—have a switch or a DSL modem built in. Some even have built-in firewalls to give your network an extra layer of protection. (For more information on routers, see the sidebar, "Which Router?")

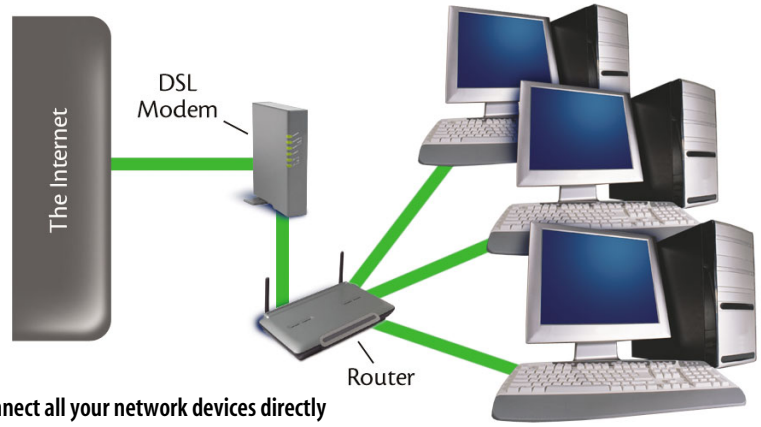
The last term you need to know is a **gateway**, which is the computer or device (such as a router) that's used to connect your home network to the Internet.

Internet Connection Sharing

Did you get all that? Then you're ready to tackle the first—and simplest—method of DSL sharing, using Windows ICS.

ICS can be used to share any type of Internet connection, including DSL, cable, and plain old analog modems. It's a standard feature on nearly all Windows machines, including Windows 98 Second Edition, Windows Me, Windows 2000, and Windows XP. In fact, that's its first benefit—it's free. It's also easy to use, fast to set up, and needs no extra equipment.

But there are drawbacks. With ICS, you'll install your DSL modem on a single computer on your network; this computer (called the host) acts as the gateway. Your home network's other computers route their Internet traffic through the gateway, which in turn routes it to your DSL modem. Hence the gateway has to be turned on for other computers to access the Internet. And if the gateway has problems—say, if Windows crashes—then other computers won't have access to the Internet. The extra traffic can also strain the gateway, making it slower or even causing it to crash if the traffic load is extremely large. Thus ICS is best for a home or small office network that comprises a small number of computers.



You can connect all your network devices directly to a router, which in turn connects to the Internet.

Using ICS

ICS varies slightly from one version of Windows to another, but the most recent version on WinXP is far and away the best. It's more stable than other versions and has special features, too, such as letting you turn a gateway's Internet connection on and off from a client machine. (This is useful if you pay for DSL by the minute or hour, as opposed to a flat rate for all-you-can-eat bandwidth.)

To install ICS on the gateway computer with WinXP, click Start, Control Panel, Network Connections, Set Up A Small Or Home Office Network. This will launch the Network Setup Wizard. Now click Next twice and then select the box marked This Computer Connects Directly To The Internet. Click Next again. You'll be prompted to select an Internet connection; choose the one you set up when you installed your DSL modem on this computer and click Next.

The wizard will prompt you to enter a computer and workgroup name. Because you've already set up your network, your computer and workgroup already have names. Be sure to enter them here exactly as you did when they were first specified, as different names will cause your network to malfunction.

Now click Next twice and Windows will get to work, setting up the gateway to let other computers use its DSL connection. When finished, the wizard will prompt you to make a setup disk to use on the client machines (that is, other PCs on the network). Click the box next to Create A Network Setup Disk option, then click Next. Load a floppy diskette into the drive, click Next, and wait for Windows to copy data to the disk. When it's done, click Next, then Finish to complete the wizard. You may be asked to restart your computer. Note that you do not have to create a setup disk if the other PCs in the network use WinXP. You can simply run the wizard on the other WinXP system.

Now it's time to set up the client machines. Just insert the setup disk

into the floppy drive of a client machine. Then click Start, Run. Type **A:\netsetup.exe** and click OK. Windows will configure the client machine to access the shared DSL through the gateway. Simply follow the wizard and restart when prompted.

ICS is easy to use because you only need to run a wizard to set up DSL sharing, and you don't have to tweak or tinker with network settings. But a word of caution: When you run the wizard on the gateway, it can make the machine's network settings conflict with your current network, causing the gateway to lose its network connection briefly. But the connection will be restored when you run the setup disk on the client machines.

Ready For A Router?

ICS is a quick and easy way to share your DSL, but it's only good for small networks that have no more than five computers. In fact, a small network with only three computers can be too much for ICS if you have lots of large downloads, if you're a gamer with a craving for high-bandwidth thrills, or if you simply demand the highest performance from your PCs.

In those cases, it's best to use a router to share your DSL connection. A router is faster and more efficient than using ICS but is more expensive. A simple router costs less than $100, but more complex routers with a built-in switch or DSL modem can make a real dent in your wallet. A wireless router can add even more to the price.

But there are good reasons to incur a router's expense. Routers do away with using a network computer as the gateway, which speeds up your network and makes it more stable. How? You can connect a router directly to your existing network's hub or switch. You then connect your DSL modem directly to the router. (Alternatively, if your router has enough ports, you can skip the switch altogether and simply connect everything to the router.) Because all the computers on your network are connected to the hub or switch at all times, they're also connected to the router and through it, to the DSL modem and the Internet. Thus you don't have to worry about keeping a host computer up and running, because there's no host computer at all.

If your router has a built-in switch and a DSL modem, it's even simpler. All the computers on your network connect directly to your router, which then connects directly to the Internet. There's only one device to worry about. For reference, see the diagrams in this article.

Set Up A Router

If the router you bought has a built-in switch and DSL modem, simply use it to replace the hub or switch that's currently used to network your home or small office. The installation will vary from router to router, so you'll need to consult your router's user guide for details. Most often, though, you'll plug the router into a single computer using a standard network cable, then insert the router's CD-ROM into that computer and run the setup program to configure the router. Once that's done, you'll plug the remaining computers on your network into the router (or access them wirelessly if you have a wireless router).

On the other hand, if your router does not have a built-in switch or DSL modem, you'll have to connect it to the hub or switch that was used to establish your home or small office network. Then you'll plug your DSL modem into the router. This type of configuration can be a bit tricky, so it's best to consult a network specialist to help with the details.

If you're an intrepid network user, you can brave the user guides for the switch, the router, and the DSL modem to make it all work together. But most of today's switches, routers, and DSL modems come with software that auto-installs and auto-configures them, so installation may not be as hard as it seems.

A little elbow grease, not to mention some brain power, will make your network work in a fairly short time, and that effort will pay off. Shared DSL can turn a home or small office network into a powerful tool for work, research, and play, bringing the Internet's wonders right to your desktop. RS

BY DAVID GARRETT

Which Router?

Choosing a router can be hard. There are many options to choose from, and the price varies widely.

First, decide if you need a router with a built-in switch or DSL (Digital Subscriber Line) modem. They're convenient because they pack the functions of three devices—a router, a switch, and a DSL modem—into a single case. That's less setup time and hassle.

If you already have a DSL modem and just want a router to attach to it, be sure to check the router's ports. Most routers will only connect to DSL modems using a standard network cable. If your DSL modem has a USB cable, be sure to find a router that allows that type of connection.

Last, decide on a wired or wireless router. A wireless router gives you the freedom to roam through your home or small office if you have a notebook computer with a wireless card. And wireless barely affects your speed, so you won't see a big difference in downloads.

Just remember that more features bring a higher price, so watch your wallet when you go shopping.

Share Your Broadband Internet Access

Cable Modems Provide Fast Connections

If you're planning to switch from dial-up to cable Internet access, you're not alone. It's no secret that dial-up Internet is painfully slow in comparison to broadband alternatives, such as DSL (digital subscriber line) and cable. After all, your modem maxes out at about 53Kbps (kilobits per second), and that's only if there isn't any signal degradation from shoddy phone wires. Cable and DSL connections, on the other hand, offer speeds up to 5Mbps or even more (cable can transfer data at even faster speeds, but you won't find 30Mbps [megabits per second] transfer rates in real-world use).

That extra speed is especially important today, as users transfer large files over the Internet on a regular basis. Particularly tech-savvy users often download large drivers for their hardware, but even casual Web surfers find themselves shuffling huge amounts of data across the Internet. People transfer picture files and homemade movies to Web sites and friends, and software publishers often distribute program updates (and sometimes entire programs) via the Internet. Even Windows Update sometimes offers large downloads for your operating system.

You can use a dial-up modem to transfer data, of course, but you must be willing to let your PC tie up your phone line for hours on end. If you're sick of waiting for Web pages to appear on your screen, you're going to love cable Internet access. Of course, there's no need to hog all the fun—you can easily share the high-speed access among all of the PCs on your existing home network. We'll show you how to connect your network to the Internet over the same cable line that feeds your

TV. Be sure to sign up for cable Internet service before you attempt to connect the cable to your network, as your cable TV subscription doesn't include Internet access. Your ISP (Internet Service Provider) may give you information about your Internet connection, such as your IP (Internet Protocol) address. Write down this information, as you may need it later.

Gear Up

Your computer's dial-up modem won't work with your cable connection, nor will your PC's Ethernet card. You'll need to install a cable modem, which transfers Internet data along the cable TV line. Chances are your network already has the other critical Internet-sharing component: a router.

Cable modem. The cable that enters your home houses many channels at 6MHz. Your cable modem requires two channels. One of the channels handles downstream data traffic (data that travels from the Internet to your computers); the other, often smaller, channel moves the upstream traffic (which is headed from your PCs to the Internet). The cable modem is responsible for assigning these channels and the data transfer. In general, you can download data faster than you can upload it, as cable providers dedicate less of the cable to upstream data. When the cable modem debuted, many cable modems used the TV cable to download data, but used a phone line to upload data to the Internet.

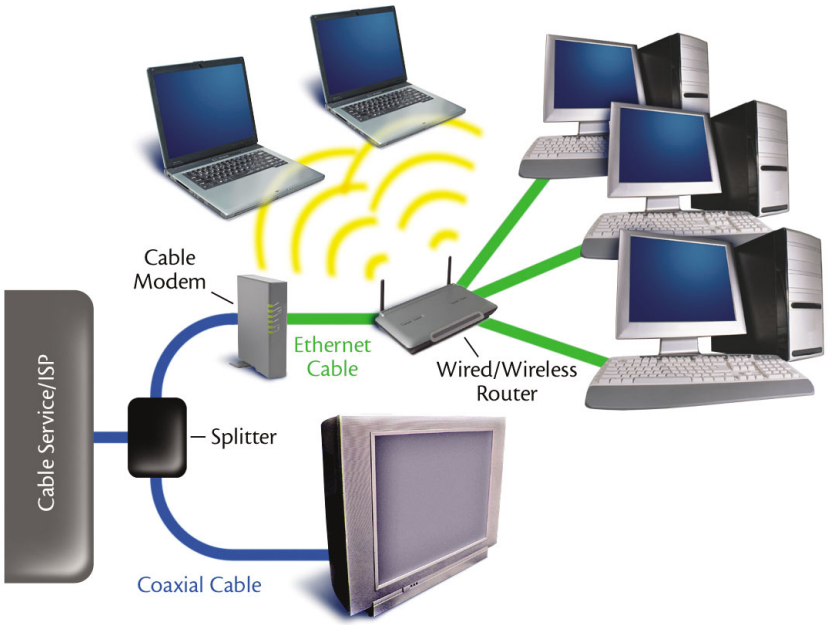
From a user's point of view, cable modems aren't very complicated. You'll find only a few interfaces at the back of the device. The coaxial connector (which looks no different than the cable connector at the back of your TV) accepts the incoming cable. The modem also has a standard RJ-45 jack (Ethernet port) and may also include a USB-B port, which resembles the letter D, rather than the more common, rectangular USB-A port. You can use either an Ethernet cable or a USB cable to connect the cable modem to your network. You may also find a reset button, which forces the cable modem to reconnect to the ISP.

Router. Your router is the lone connection between your home network (your PCs and printers) and the Internet. All of your network PCs connect to your router, either via

Ethernet cables or wirelessly, to access the cable's Internet connection. The back of your router includes a WAN (wide-area network) port that lets you connect the router to your cable modem via a standard Ethernet cable.

Today's routers have a ton of extra features that enhance and protect your network. Many have a built-in switch that includes several Ethernet ports. If you have more wired network computers than the router has ports, you'll need to add an additional switch (which provides more ports) to the mix. Some routers also have wireless technology, such as 802.11b or g, which lets them add your wireless PCs to your network.

Because the router is the last stop that data makes before reaching your PCs (or reaching the Internet, depending on the direction the data is going), it's a great place to throw up some defenses against malicious users and snoops. To that end, routers often have built-in hardware firewalls that provide a shield for your network. Routers also often use NAT (network address translation) to hide your network's computers behind the router so that the router is the only device in your network visible to the Internet.



Your TV cable can provide high-speed Internet access that blows the roof off of dial-up's agonizing data trickle, but you can't access the Internet until you sign up for the service from your ISP (which may also be your cable TV provider). The ISP service person will attach a splitter to the end of your cable. The splitter divides the cable's channels, so that the TV channels continue, uninterrupted to your TV. Once the Internet data passes from the cable to the splitter, it heads down a different cable to your cable modem, which translates the signal and then passes it to your router. Your router then distributes Internet access to all of your network's PCs.

Attach Your Cable Modem To The Network

Chances are, your ISP offers a cable modem installation service and can also supply you with a cable modem. Some ISPs loan the modem as part of the service, others rent them to customers. However, you may prefer to buy your own cable modem and install it yourself.

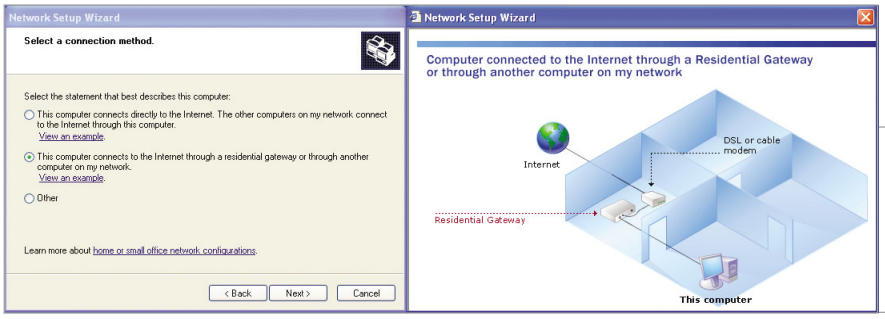
If you choose to buy and install your own cable modem, expect to spend about $50 to $75 on the modem. You'll also need to buy a splitter (something your cable service person would provide during the installation), which has three coaxial plugs. One accepts the incoming cable, another directs the cable to your TV, and a third directs your cable to your network.

Once you've installed the splitter, you can screw the cable onto the modem's connection. Next, plug an Ethernet cable into the modem and the router's WAN port. If your router isn't already a part of your network, connect your PCs to the router's LAN (local-area network) ports.

Once you power on your cable modem and your router, check your PCs to see if they can connect to the Internet. In many cases, the router automatically shares the Internet connection. If not, you may need to configure your router to accept and share the Internet connection.

Configure Your Router

Open your router's configuration menu (you may need to enter the

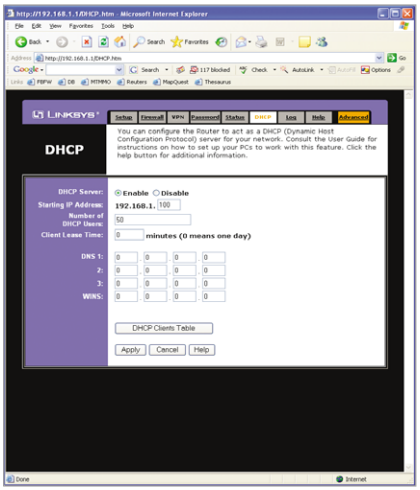

Network Setup Wizard
Select a connection method.
Select the statement that best describes this computer:
This computer connects directly to the Internet. The other computers on my network connect to the Internet through this computer.
View an example.
This computer connects to the Internet through a residential gateway or through another computer on my network.
View an example.
Other
Learn more about home or small office network configurations.
< Back
Next >
Cancel
Network Setup Wizard
Computer connected to the Internet through a Residential Gateway or through another computer on my network
Internet
DSL or cable modem
Residential Gateway
This computer

The Windows Network Setup Wizard configures your computers to share files, printers, and Internet access. Run this wizard on each computer in your network.

router's IP address in a Web browser in order to access the menu—check your manual) and then fill in any information that your ISP provided. If your ISP doesn't provide an IP address, host name, or domain name, set your router to automatically obtain an IP.

Next, make sure that DHCP (Dynamic Host Configuration Protocol) is enabled. DHCP and NAT assign IP addresses to all of the PCs in your network but hide the PCs (and these temporary IP addresses) behind the router's IP address. As a result, your router is the only connection to the Internet, regardless of the number of PCs on your network. While you're in this menu, consider reducing the number of allowed DHCP users to match the number of PCs on your network. This will help ensure that snoops can't break into your network.

You'll also want to make sure that your PCs are configured to support DHCP. For each Windows XP PC, click Start, My Network Places, and then click View Network Connections in the Network Tasks menu that appears in the left side of the window. Right-click Local Area Connection and then click Properties. Click TCP/IP and then click Properties. Click the Obtain An IP Address Automatically radio button and then click OK. Your computers should now have Internet access.



Use your router's configuration menu to enable DHCP. You can bolster your network's security by limiting the number of DHCP-based addresses to match the number of users on your network.

Run The Network Setup Wizard

If you're just installing your router now, you'll need to run the Windows Network Wizard so your network can share files and printers. To start the wizard, choose one of your WinXP PCs and then click Start, All Programs, Accessories, Communications, and Network Setup Wizard.

Click the Next button when the Welcome To The Network Setup Wizard page appears and then click Next again when the Before You Continue page appears. Click the radio button next to This Computer Connects To The Internet Through A Residential Gateway Or Through Another Computer On My Network. (The View An Example link displays an image of a router that sits between your cable modem and a PC on your network.) Click Next.

The next two pages ask you to name your PC and your network's workgroup name. By default, Windows provides the workgroup name MSHOME. You can choose any name, but be sure to enter that same workgroup name onto each PC you put on this network. Enable file and printer sharing when the relevant page appears and then review the settings you've chosen. You may want to write down these settings, as you'll need to choose the same settings on each PC in your network. Finally, click Next. The wizard will apply the settings. If all of your computers have WinXP, you can finish the wizard and then move to the next PC. If you have PCs running older OSes, you can use the wizard here to create a setup disk for the older systems.

Smooth Sailing

Now that your network has shared, always-on Internet access, it's important that your PCs are well-protected. Double-check your PCs to make sure they have the latest OS, antispyware, and anti-adware updates. You'll also want configure your router's wireless feature so that it encrypts communications with your notebooks (see our Security section to learn more about wireless encryption). Without the protection that encryption and firewalls provide, your Internet access may change from boon to curse. RS

BY JOSHUA GULICK

When In Doubt, Reset

If you run into trouble sharing your cable Internet connection with your network, try resetting your cable modem. Some cable modems have reset buttons. If you see a reset button, press it and hold the button for several seconds to perform the reset. Your cable modem may use its activity LEDs to indicate that it has reset; check your manual to learn about the modem's LED codes. A cable modem that doesn't have a reset button isn't unresetable; power it off and wait for a minute or so. When you power on the modem, it will reacquire its connection to your ISP and (hopefully) begin the data shuffle.

If the cable modem reset doesn't do the trick, reset your cable modem *and* your router (keep in mind that when you reset your router, it may revert to the default password, in which case you'll need to reset the password as well). In our experience, we've found that you can sometimes breathe life into your network by shutting down all network computers, the router, and the cable modem, and then powering on the devices (first the cable modem, then the router, then the network PCs).

Share A Dial-Up Connection

Old-School Networking

In spite of the prevalence of broadband (cable or DSL [Digital Subscriber Line]) connectivity today, the fact remains many PC users still rely on trusty ol' dial-up connectivity to access the Internet. If you simply use the Internet to check email and browse the occasional Web site, then dial-up connectivity is a perfectly acceptable way of getting online without having to pay broadband prices.

Even if you're still using dial-up to access the Internet, chances are you have more than one computer in your household. If that's the case, you can set up Microsoft Windows to share that dial-up Internet connection among all your computers. Read on to learn more about using ICS (Internet Connection Sharing) to share your dial-up connection.

The Basics

ICS is a Windows feature—first appearing in Windows 98 Second Edition—that allows a single Internet connection to be shared among multiple computers. ICS does this by using a designated computer, called the host (or gateway) to perform the networking functions that are typically done by other hardware devices used in networking, such as routers. These functions include DHCP (Dynamic Host Control Protocol), NAT (Network Address Translation), DNS (Domain Name Server) proxy, and others.

To use ICS, you set up a PC as the host and install and configure ICS on that PC. The only caveat here is that this host PC must run Win98SE or later; the other PCs in your network, however, can run any version of Windows and work well with ICS.

It's important to keep one fact in mind before you proceed: When multiple PCs access the same dial-up connection, those systems will experience slower connectivity because ICS shares the available bandwidth among all computers. If this is a problem, it may just be the impetus you need to graduate to a broadband connection. Now, let's take a look at how to set up ICS to share a dial-up connection.

Prepare To Share

Before you begin, it's a good idea to know how your network will be configured and how your client and host PCs will connect to each other. A switch or hub is an easy way to connect all of your client PCs to your host PC, which is in turn connected to the Internet (in this case, via a dial-up connection).

To connect to your network, your host and client PCs will all need NICs (network interface cards). Even though the host connects to the Internet via a dial-up connection, it will still need a NIC to connect to the hardware switch or hub that is in turn connected to all the other computers in your network.

Once you have everything hooked up, it's a good idea to check the network settings for each of the PCs. (*NOTE: these instructions are for PCs running Windows XP.*)

To check your network settings, click Start, Control Panel, and then Network And Internet Connections. Then, click the Network Connections icon at the bottom of the Network And Internet Connections window.

When checking your host PC's connection, you will see, at least, a Dial-Up icon and a Local Area Connection icon in the Network Connections window. The dial-up connection connects to the Internet and the LAN (local-area network) connects your host PC to the other PCs in your network. Check the properties of your LAN connection on each PC by right-clicking the Local Area Connection icon in the Network Connections window and clicking Properties.

In the General tab of the Local Area Connection Properties window, you should see your NIC listed in the Connect Using text box. Also, in the This Connection Uses The Following Items list box, you should see a number of clients and protocols listed.

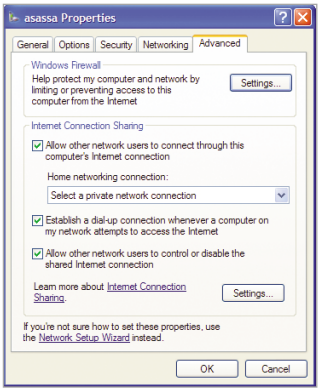
For a working LAN connection, you should see Client For Microsoft Networks, File And Printer Sharing For Microsoft Networks, and Internet Protocol (TCP/IP) listed here. If any of those items are missing, click the Install button and follow the instructions to install them. You may need your Windows installation CD to do this.

Once you verify all of your network connections in your host and client computers, it's time to set up your host PC for ICS.

Set Up The Host

Here's a not-so-obvious step you should take before you set up ICS on the host PC: Verify that all of the settings, such as the phone numbers and dialing rules, are correctly set up on your host PC's dial-up connection.

To begin setting up the host to share a dial-up connection, click Start, Control Panel, and Network And Internet Connections. If you're using WinXP's Category View, click Network And Internet Connections; if you are in Classic View, double-click Network Connections.


asassa Properties
General
Options
Security
Networking
Advanced
Windows Firewall
Help protect my computer and network by limiting or preventing access to this computer from the Internet
Settings...
Internet Connection Sharing
Allow other network users to connect through this computer's Internet connection
Home networking connection:
Select a private network connection
Establish a dial-up connection whenever a computer on my network attempts to access the Internet
Allow other network users to control or disable the shared Internet connection
Learn more about Internet Connection Sharing.
Settings...
If you're not sure how to set these properties, use the Network Setup Wizard instead.
OK
Cancel

When configuring your dial-up connection for ICS, be sure to choose the Allow Other Network Users To Connect Through This Computer's Internet Connection option.

Clicking Network And Internet Connections in Category View opens the Network And Internet Connections window. In this window, click the Network Connections icon at the bottom to open the Network Connections window. If you are in Classic View, double-clicking the Network Connections icon in the previous steps opens the Network Connections window.

In the Network Connections window, you should see an icon for your dial-up connection. To set up ICS on this connection, right-click the icon and click Properties. Doing this opens the Properties window for your dial-up connection.

In the General tab of this window, you should see your modem listed in the Connect Using textbox and the phone number for your ISP (Internet service provider) in the Phone Number option group. Click the Advanced tab. Here you'll see an option group for Internet Connection Sharing.

First, click the Allow Other Network Users To Connect Through This Computer's Internet Connection checkbox. If you have more than one LAN connection, you will see these listed in the Home Networking Connection drop-down box. Select the LAN icon you use to connect the host to the client computers in your network.

Next, click the Establish A Dial-Up Connection Whenever A Computer On My Network Attempts To Access The Internet checkbox. This launches the dial-up connection in your host PC when one of the clients attempts to access the Internet. If you don't select this option, you'll have to establish the dial-up connection manually when one of your PCs attempts to connect.

Finally, click the Allow Other Network Users To Control Or Disable The Shared Internet Connection checkbox. This will let a user on a client PC disconnect the dial-up connection whenever they finish using the Internet. Click OK to accept your changes and then follow any subsequent instructions.

Set Up Your Clients

Now that ICS is set up on your host computer, it's time to set up the client computers. To do so, use the Network Setup Wizard. If your client computers run WinXP, launch the Network Setup Wizard by clicking Start, All Programs, Accessories, Communications, and Network Setup Wizard.

If your client PC runs Windows 98, Win98SE, or Windows ME, you can run the Network Setup Wizard by either using the WinXP installation CD or using a network setup disk created during a previous ICS setup session. If you're using the WinXP CD, insert the CD in the client PC's CD drive. When the WinXP setup screen appears, click the Perform Additional Tasks option and then click Set Up A Home Or Small Office Network when prompted. If you're using a floppy diskette that has the Network Setup Wizard, insert the disk into your drive, then click Start, Run, and type **A:\Netsetup** in the textbox to launch the wizard.

Click Next at the wizard's welcome screen to start, and click Next again to advance past the Before You Continue screen. In the Select A Connection Method screen, click the This Computer Connects To The Internet Through A Residential Gateway Or Through Another Computer On My Network radio button.

Next, select the connection you use to connect to the host by clicking the appropriate checkbox in the Connections list box and click Next. In the following screen, the wizard asks you to give the client computer a name; enter a unique name in the Computer Name textbox and a description (this step is optional) in the Computer Description textbox. Click Next when finished.

In the next screen, the wizard asks you to name the network with a workgroup name. Click Next to advance. In the next screen, the wizard lists the settings you chose. Click Next to advance.

When the wizard's done, it'll ask if you want to create a Network Setup Disk or if you want to use the WinXP CD-ROM to set up ICS on other clients. If you don't want to do either, click the Just Finish The Wizard radio button. The final screen says you have successfully set up the client for networking, so click the Finish button to complete the process. You're done!

Share The Wealth

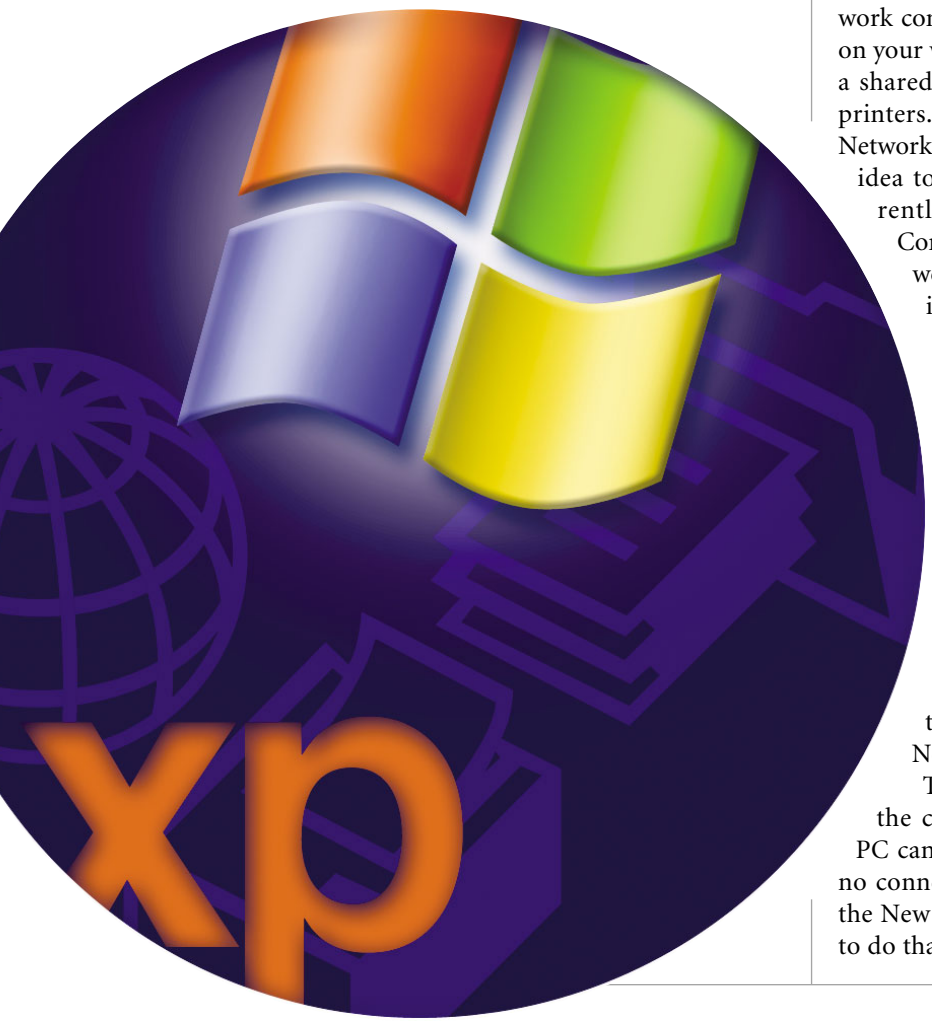
ICS provides you with a straightforward way to share a dial-up connection among multiple computers. The key to successfully setting up a dial-up network is to do a little preplanning before you begin. RS

BY SIXTO ORTIZ

WinXP Networking Wizards & Settings

Where To Go For Networking Help

The good news is that setting up and managing a network is easier in Windows XP than any other Microsoft operating system. The bad news is that there are still a lot of choices to make and things that can go wrong. We'll walk you through using the WinXP networking wizards, show you how to manage your current networking settings, and talk about the differences between the various flavors of XP.



Find The Windows XP Network Tools

If you haven't already set up a network with WinXP, there are several wizards that can help you get your network started. The majority of WinXP's networking tools are available in your My Network Places system folder. It's easy enough to open up this folder—just click Start and then select My Network Places.

From this folder, you can view your current network connections, see the other computers that are on your workgroup, jump to other locations such as a shared files folder, or view available networked printers. You can create a new network from My Network Places, but before we start that, it's a good idea to see what network connections you currently have available. To get to the Network Connections system folder, click the View network connections item under Network Tasks in the My Network Places folder. (*Note: If these tasks don't appear, click the double Down arrows next to Network Tasks.*)

You can also get to the Network Connections system folder by right-clicking on any network icon in the System Tray and selecting Open Network Connections from the pop-up menu. This folder is also accessible as an icon in the Control Panel. And because Windows always has plenty of paths to the same destination, we'll give you one more. Click Start, select Connect To, and then select Show All Connections and the Network Connections folder will open.

The Network Connections folder shows the connections currently available that your PC can use to connect to a network. If there are no connections available, you can create one with the New Connection Wizard. We'll show you how to do that next.

Use The New Connection Wizard

The New Connection Wizard supports a variety of connections, from dial-up and broadband to VPN (virtual private network) and direct connections to another PC. You can access the New Connection Wizard from the Network Connections folder by clicking Create A New Connection under Network Tasks.

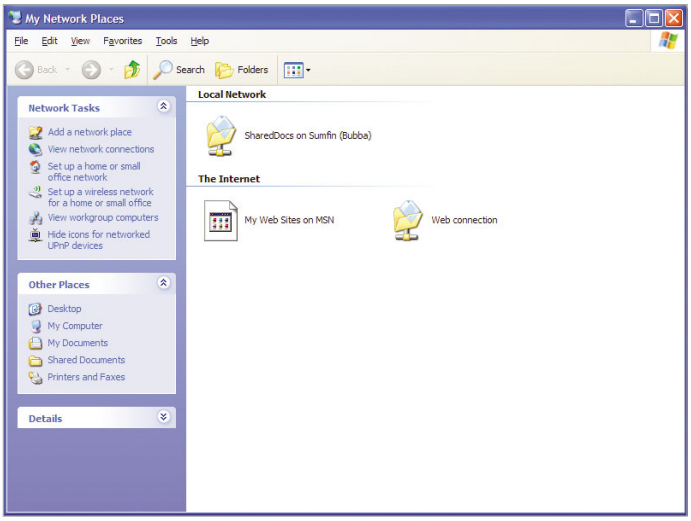
The first page of the wizard offers a hearty welcome and explains what the New Connection Wizard can do. Clicking Next will bring you to the page where you decide which type of connection to create. The wizard can help you create a connection to the Internet, to your workplace network, to a small office or home network, and to another PC directly via a serial, parallel, or infrared port. This last option isn't used as much as it used to be, but some users still find the need to connect two systems directly.

If your New Connection Wizard only offers you three choices on this page, you might not have installed Service Pack 2 to your WinXP operating system. We highly recommend the SP2 upgrade before networking your XP system, as this service pack includes a lot of improvements to the XP networking tools.

The first option is creating an Internet connection. You can use this option to create a new dial-up or broadband connection. Because this article deals with networking WinXP systems, we won't walk through the details of creating a brand-new connection to the 'Net.

Connecting to your workplace network is the second option. You can connect to your network remotely by directly dialing into the network or via VPN. You'll need to know the number you dial or the name of the VPN server (either the domain name or the actual IP address) and the process takes only a couple of steps to fill in this information. You also have the option of creating a shortcut to your office network on your Desktop with this wizard so in the future you only need to double-click that shortcut to connect.

Choosing the third option will close the New Connection Wizard and open up the Network Setup Wizard, which we will get to in a moment.



The My Network Places system folder is the central repository for most of the Windows XP tools you'll use to set up your network.

Finally, the fourth option walks you through the process of creating a direct cable connection between two systems. This part of the wizard takes you through the steps of connecting a cable between two ports on these systems and lets you choose who can connect to your system and how they can do it.

Set Up A Network

The most robust wizard for WinXP networking is the Network Setup Wizard. It can help you share an Internet connection between two or more systems, share a printer or files among multiple systems, and even set up a firewall to protect your network from unwanted entry. To start the Network Setup Wizard, click Set Up A Home Or Small Office Network under Network Tasks in either the My Network Places or the Network Connections system folder.

Click Next on the welcome page that you see when you open the Network Setup Wizard. The second page has a link to WinXP's checklist for creating a network. This checklist states all the choices and considerations you need to make before setting up a network. These include the layout, or topology, of the network, which computer you want to use as the host for (ICS) Internet Connection Sharing, what additional hardware or cabling you might need for your network, and the basic steps to follow for setting up the network. It's a good idea to familiarize yourself with this checklist before continuing to set up your WinXP network.

After you've completed the checklist, run the Network Setup Wizard again. Make sure that all computers and devices you want to network are turned on and connected to one another and that your host computer for ICS is connected to the Internet, and then click Next. If the wizard finds disconnected hardware on the PC you're running it on, you may see a page telling you about it. You can check the Ignore Disconnected Network Hardware box and then click Next if the hardware isn't needed for this network.

The next page lets you describe how your computer connects to the Internet. You should be running the Network Setup Wizard on your host computer that directly connects to the Internet, so leave the first option checked and click Next.

The following page lists the Internet connections you have available and lets you choose which one you use to connect to the Internet. In most cases, WinXP will preselect

the correct connection, so you can just click Next.

The next page lets you enter a description and a name for your PC. The description is for your benefit only—you can enter anything you like, such as the room that the computer is in or the name of the primary user. But the computer name can be important. Your ISP (Internet service provider) may want to have a specific name for your computer when it logs in to its server. In that case, leave the name that appears in the Computer Name field.

Clicking Next takes you to a page where you'll name your network. The default network is MSHOME, but you can name your network whatever you'd like. But remember the name you choose as you'll need to enter it into the Network Setup Wizard on your other computers. Click Next.

The following page lets you decide whether to enable file and printer sharing with other systems on your network. To allow this, click the radio button labeled Turn On File And Printer Sharing. If you're not sure if you'll need to share files or printers over your network, click the radio button in front of Turn Off File And Printer Sharing. You can always enable one or both of them later, and your network will be more secure with file sharing off. Click Next when you're done.

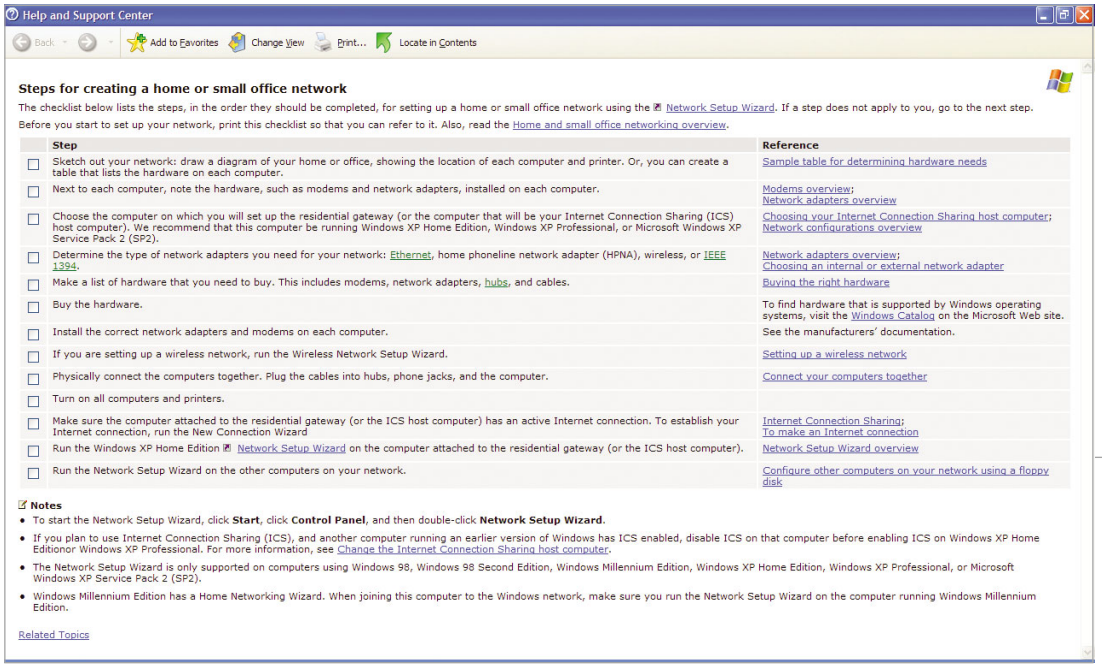
The next page shows you all of the settings that will be applied. ICS and the Internet Connection Firewall will be turned on, as well as file and printer sharing if you selected that option previously.

After the configuration process is completed, the Network Setup Wizard will help you prepare to run it on your other systems. On systems that aren't running WinXP, you can run the Network Setup Wizard from the WinXP CD. If you have a non-XP system with only a floppy drive, you can select the option to create a Network Setup Disk at this point. Select the option you want and click Next. The final page just tells you that you have successfully completed the Network Setup Wizard. Click Finish and you're done with your host PC.

If you wish to use the WinXP CD on non-XP systems, here are the steps to follow: Insert the CD into the CD-ROM drive, select Perform Additional Tasks in the menu that appears, and then click Set Up Home Or Small Office Networking. A WinXP network is non-exclusive. It lets Windows ME, Windows 98, and computers running other operating systems onto the network after you run the Network Setup Wizard on these systems.

Now you need to run the Network Setup Wizard on any WinXP PCs that you will have on your network. Leave your host PC on and connected to the Internet as you complete this process. On the Internet Connections page, select the option that says This Computer Connects To The Internet Through Another Computer On The Network. Also, be sure to enter the same network name that you did on your host computer if it doesn't automatically appear. After you have run the Network Setup Wizard on all of your networked PCs, your network is ready to go.

You can view the other computers on your network by clicking Start and selecting My Network Places. Under Local Network, you'll see the Shared Documents folders of all the systems on your network, which makes it easy to move files back and forth between your connected PCs if you've enabled file sharing. The Shared Documents folder for each PC is located in the My Computer system folder. To access this folder, click Start and select My Computer. Any files or folders you place in this folder can then be accessed across the network.


Help and Support Center
Back
Add to Favorites
Change View
Print...
Locate in Contents
Steps for creating a home or small office network
The checklist below lists the steps, in the order they should be completed, for setting up a home or small office network using the Network Setup Wizard. If a step does not apply to you, go to the next step.
Before you start to set up your network, print this checklist so that you can refer to it. Also, read the Home and small office networking overview.
Step
Reference
Sketch out your network: draw a diagram of your home or office, showing the location of each computer and printer. Or, you can create a table that lists the hardware on each computer.
Sample table for determining hardware needs
Next to each computer, note the hardware, such as modems and network adapters, installed on each computer.
Modems overview; Network adapters overview
Choose the computer on which you will set up the residential gateway (or the computer that will be your Internet Connection Sharing (ICS) host computer). We recommend that this computer be running Windows XP Home Edition, Windows XP Professional, or Microsoft Windows XP Service Pack 2 (SP2).
Choosing your Internet Connection Sharing host computer; Network configurations overview
Determine the type of network adapters you need for your network: Ethernet, home phoneline network adapter (HPNA), wireless, or IEEE 1394.
Network adapters overview; Choosing an internal or external network adapter
Make a list of hardware that you need to buy. This includes modems, network adapters, hubs, and cables.
Buying the right hardware
Buy the hardware.
To find hardware that is supported by Windows operating systems, visit the Windows Catalog on the Microsoft Web site.
Install the correct network adapters and modems on each computer.
See the manufacturers' documentation.
If you are setting up a wireless network, run the Wireless Network Setup Wizard.
Setting up a wireless network
Physically connect the computers together. Plug the cables into hubs, phone jacks, and the computer.
Connect your computers together
Turn on all computers and printers.
Make sure the computer attached to the residential gateway (or the ICS host computer) has an active Internet connection. To establish your Internet connection, run the New Connection Wizard
Internet Connection Sharing; To make an Internet connection
Run the Windows XP Home Edition Network Setup Wizard on the computer attached to the residential gateway (or the ICS host computer).
Network Setup Wizard overview
Run the Network Setup Wizard on the other computers on your network.
Configure other computers on your network using a floppy disk
Notes
To start the Network Setup Wizard, click Start, click Control Panel, and then double-click Network Setup Wizard.
If you plan to use Internet Connection Sharing (ICS), and another computer running an earlier version of Windows has ICS enabled, disable ICS on that computer before enabling ICS on Windows XP Home Editionor Windows XP Professional. For more information, see Change the Internet Connection Sharing host computer.
The Network Setup Wizard is only supported on computers using Windows 98, Windows 98 Second Edition, Windows Millennium Edition, Windows XP Home Edition, Windows XP Professional, or Microsoft Windows XP Service Pack 2 (SP2).
Windows Millennium Edition has a Home Networking Wizard. When joining this computer to the Windows network, make sure you run the Network Setup Wizard on the computer running Windows Millennium Edition.
Related Topics

Windows XP offers a handy checklist to make sure you have all the hardware and software components necessary for creating a network.

Set Up A Wireless Network

A new Network Task added with Service Pack 2, the

Wireless Network Setup Wizard is a modified version of the Network Setup Wizard that helps you create a wireless home or small office network. To start this wizard, open the My Network Places system folder and click Set Up A Wireless Network For A Home Or Small Office under Network Tasks.

Clicking Next on the welcome page takes you to a page where you can name your wireless network (up to 32 characters in the Network Name text field, also called the SSID [Service Set Identifier]), and set up wireless security. The wizard can automatically create a security key for your new network if you check the radio button in front of Automatically Assign A Network Key. If you already have a wireless network with a network key, check the button in front of Manually Assign A Network Key.

The Wireless Network Setup Wizard uses WEP (Wired Equivalent Privacy) as the default security mode, the original security protocol for wireless networks. You can also opt for the newer WPA (Wi-Fi Protected Access), a stronger encryption standard, if you know all your networking hardware support this standard. Any PCs with WinXP Service Pack 1 or later incorporate WPA support.

Check the documentation that came with your router or other device to see if it supports WPA. To enable WPA, click the box in front of Use WPA Encryption Instead Of WEP at the bottom of the page. Click Next when you're finished.

The next page asks you how you want to set up your wireless network. The recommended option is to create the settings and then transfer them to a USB flash memory drive. Of course, this requires you to have a USB flash drive. If not, you can recreate the settings manually on each computer. Choose the appropriate option and click Next.

If you chose the manual option, you'll see a button that prints out your wireless network settings so they're easier to enter into each device. The wizard recommends entering your settings into the main access point or router first, then each computer that will connect to that access point, and finally, any other wireless devices such as a wireless printer.

If you do have a USB flash drive, the wizard can transfer all your network settings to the drive. Plug it in to the PC that you just set up for wireless networking, wait for the wizard to recognize it, and click Next.

After your network settings are transferred to your flash drive, remove it and plug it into your main wireless access point. If your main access point doesn't have a USB connection, you'll have to set up the network manually. Most access points that support this form of updating will flash their status light three times to indicate that the new settings have been accepted. If not, wait 30 seconds before removing the flash drive.

Next, connect the flash drive to each of the computers that you want to connect to your network. The Wireless Network Setup Wizard will run and ask if you want to join the network. Click OK. Finally, plug the flash drive into the computer you first ran the wizard on and click Next.

The last page just shows you the devices that you have successfully set up for your wireless network. The wizard can automatically delete the network settings from your flash drive if you leave the box checked in front of For Security Reasons, Remove Network Settings From My Flash Drive. Click Finish to close the wizard and your wireless network should be up and running.

Share Files & Folders

Even if you opted to share the default folder during network setup, you can share additional folders across your network as well. To share any folder, simply highlight the folder by clicking it once and then select Share This Folder under File And Folder Tasks. Alternatively, you can right-click a folder and select Sharing And Security from the pop-up menu.

If you declined to turn on file and printer sharing when you ran the Network Setup Wizard, you might see a notice asking you to run it again before you can share additional folders from the Sharing tab. You can also click the link below that says you want to skip this step.

Afterwards, you'll be able check the box in front of Share This Folder On The Network in the Network Sharing And Security section of the Sharing tab. You can type a new name for the

Windows Media Center Extender

Windows XP Media Center Edition features the ability to extend your computer's network to your television or portable devices. For example, if you have an Xbox 360, you can access files on your PC from the Xbox, viewing photos and video on your living room TV over the network.

You can also purchase a Media Center Extender hardware device such as the wireless WMCE54AG from Linksys ($299; www.linksys.com) that works in a similar fashion, letting you access files from your Media Center PC and view them on a television or a Portable Media Center device from manufacturers such as Creative and i-River.

Finally, you can perform some of these tasks with non-Media Center versions of XP with an add-on called Windows Media Connect, available here: http://www.microsoft.com/windows/windowsmedia/devices/wmconnect/default.aspx. This add-on lets you connect your WinXP network to an Xbox 360 or other compatible digital media receiver for viewing multimedia files across the network. ❙

folder in the Share Name text field if you want to share it under a different name. And, by checking the box in front of Allow Network Users To Change My Files, you'll allow other users on the network to edit the files in shared folders. By leaving this box blank, the files will be read-only.

You can make it easier to reach this folder from another computer by mapping it as a network drive. To do this, open the My Computer folder (Start, My Computer) and then select Map Network Drive from the Tools menu. In the Drive field, select a drive letter you'd like to use for the network drive. In the Folder field, you can type the path to the shared folder if you know it, but it's probably easier to click the Browse button and find the folder that way. If you leave the Reconnect at logon box checked, this drive will automatically show up in your My Computer folder for easier access.

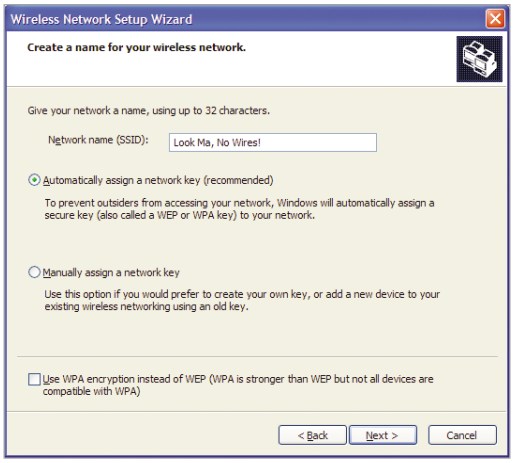
Share A Printer

If you add a new printer to your network or decide to share a printer that you originally kept private, you can opt to share it in the Printers and Faxes folder. You can access this folder by clicking Start and then selecting Printers and Faxes, or by clicking Start, Control Panel, Printers And Other Hardware, and then Printers And Faxes.

Once you've opened the Printers and Faxes folder, highlight the printer you want to share by clicking it once and then select Share This Printer under Printer Tasks on the left side of the window. Again, if you opted out of file and printer sharing during the Network Setup Wizard, you may need to run it again or click the link to skip this option. Otherwise, you'll be shown the Sharing tab of the printer's properties window. Check the radio button in front of Share This Printer and enter a name for it in the Share Name text field. If you'll be sharing it with computers that aren't running Windows XP, you can install drivers for other operating systems by clicking the Additional Drivers button and checking boxes in front of the operating systems you want to support. (*Note: you may need the driver disk that came with your printer to complete this step.*)

Windows XP Professional

The Professional version of Windows XP is fairly similar to the Home version, but there are some subtle and not-so-subtle differences in terms of networking. For example, you can allow another user to control your XP Professional system remotely, with that person's mouse and keyboard controlling the cursor of your system.


Wireless Network Setup Wizard
Create a name for your wireless network.
Give your network a name, using up to 32 characters.
Network name (SSID):
Look Ma, No Wires!
Automatically assign a network key (recommended)
To prevent outsiders from accessing your network, Windows will automatically assign a secure key (also called a WEP or WPA key) to your network.
Manually assign a network key
Use this option if you would prefer to create your own key, or add a new device to your existing wireless networking using an old key.
Use WPA encryption instead of WEP (WPA is stronger than WEP but not all devices are compatible with WPA)
< Back
Next >
Cancel

Windows XP supports both WEP and WPA encryption standards for wireless networks.

To enable this feature in XP Professional, open the Control Panel by clicking Start and selecting Control Panel. Double-click the System icon to open the System Properties. Select the Remote tab. Under Remote Desktop, check the box in front of Allow Users To Connect Remotely To This Computer. You may get a warning message, but just click OK. Now, click the Select Remote Users button and click the Add button to tell XP Professional who has the right to take control.

Windows XP Professional also supports more simultaneous file-sharing users (10 compared to XP Home's five) and has additional security features for your network, making it possible for one user to have read-only file access and another to have the ability to modify documents, for example. To make these types of changes, you can right-click any shared folder and select Properties from the pop-up menu. Click the Security tab and highlight a group or user name to change. In the Permissions pane, check or uncheck the options that you want that group or user to have. Click OK or Apply when you're finished.

Troubleshooting A Network

Setting up a network on Windows XP is a fairly straightforward process thanks to the helpful wizards that can walk you through most of the steps in the setup. But if you run into problems along the way, you can also use XP's troubleshooters and diagnostic tools. To access these utilities, click Start and select Help And Support. In the Help And Support Center that opens, click Networking And The Web. Under the Networking And The Web sidebar on the left, click Fixing Networking Or Web Problems. This will bring up a list of troubleshooters as well as the Network diagnostic tool. To access the latter, click Diagnose Network Configuration And Run Automated Networking Tests under Pick A Task. Under Network Diagnosis, click Scan Your System. The results can show you where any problems with your network may lie.

Windows XP features plenty of robust tools that make setting up and maintaining a network an easier task than it has ever been in a Windows operating system. Once you've familiarized yourself with the helpful wizards, you'll be able to set up your own wired or wireless home or small office network without much trouble. RS

BY JOEL STRAUCH

Windows 98 Networking Wizards & Settings

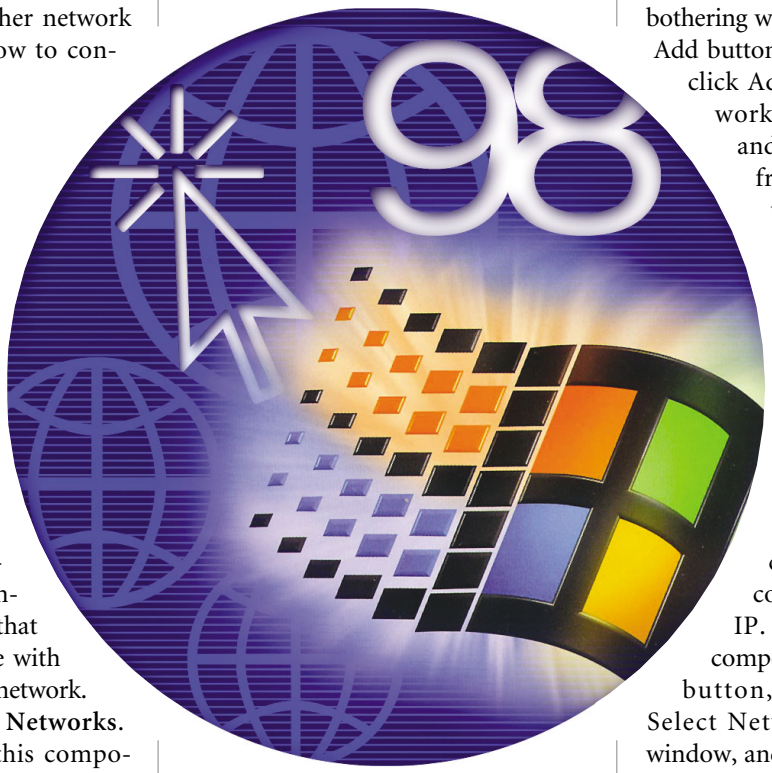
Configure Win98 To Share Folders & Printers

Although Windows 98 and Windows 98 Second Edition don't have as many networking features and wizards as newer versions of the OS, they have all the options you'll need to connect your PC to your network and share files and printers with other network users. We'll show you how to configure your Win98 PC.

Configure Your PC's Network Settings

You can access Win-98's network options by clicking Start, Settings, Control Panel, and then double-clicking the Network icon. By default, this feature opens to the Configuration tab, which displays your operating system's installed networking components. You'll need to install several components that let your PC communicate with the other systems on your network.

Client For Microsoft Networks. Chances are, you'll see this component in the The Following Network Components Are Installed field right away. It lets your computer access other computers over a network whether the network has a server or not. You don't need to change any of this component's settings. If it does not appear in the component field, click the Add button. When the Select Network Component Type window appears, select Client and then click the Add button. Select Microsoft in the Manufacturers field and then select Client For Microsoft Networks in the Network Clients field. Click OK.



Network Adapter. Whether you have a modem or an Ethernet card (also known as a network adapter), it will appear in the components field. If you don't see your network adapter in this field, you probably haven't yet installed its drivers. Your Ethernet card or modem should include a disc that has the appropriate drivers. If your motherboard has an integrated network adapter, the adapter's drivers are on the motherboard's CD.

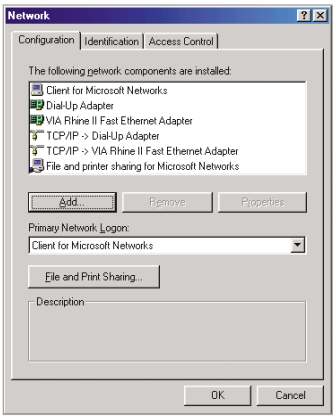
Check to see if Win98 already has drivers that will support your adapter (the OS [operating system] carries tons of drivers that you can install without bothering with a driver disk). Click the Add button, select Adapter, and then click Add. Next, select your network adapter's manufacturer and then choose the adapter from the list that appears under Network Adapters. If your adapter doesn't appear in the list, click the Have Disk button and then insert your adapter's driver disk. Follow the prompts to install your driver.

TCP/IP. Your PC needs a protocol that lets it handle your Internet connection. Check the components field for TCP/IP. If it's not already in the components field, click the Add button, select Protocol in the Select Network Component Type window, and then click Add. Next, select Microsoft from the Manufacturers field and then select TCP/IP from the Network Protocols field. Click OK.

File And Printer Sharing. If you want to share certain folders and files over your network and let other network users access your PC's printer, you'll want to enable this feature. If it doesn't already appear in the components field, click the File And Print

Sharing button and then check the two checkboxes that appear in the File And Print Sharing window. Click OK. File And Printer Sharing For Microsoft Networks now appears at the bottom of the component field.

Now that you've installed networking components for your PC, it's time to determine how your computer will appear on the network. Click the Identification tab in the Network window. The Computer Name field contains the name that will appear on your network. If you entered a user name when you installed Win98, that name may appear in the Computer Name field by default. You can keep that name or change it to a name that will let other network users more easily identify your computer. For example, you could name your computer by the room in which it sits, or the name of the person who most often uses the computer.



The Network menu houses several important networking settings, including your PC's network name and networking components.

You'll also need to choose a workgroup name. Be sure to enter the same workgroup name for each of the computers on your network: When you search for other network computers later, you can find them in this same workgroup. You can also enter a brief description of your computer in the Computer Description field. This description also helps users identify your computer. You can leave this field blank, but you will need to enter names in the Computer Name and Workgroup fields.

Next, click the Access Control tab and then click the Share-Level Access Control radio button. This feature lets you set a password for items that you share, such as folders and printers (you'll need to configure these resources' sharing properties later). You can then give the passwords to authorized network users. This feature adds some flexibility to your network security: If you want to share your printer with all network users, but want to share a particular folder with only certain users, you can create a password for each resource and then share the passwords accordingly.

Finalize your PC's new network settings by clicking the OK button at the bottom of the Network window. A Copying Files window may appear briefly as your PC pulls related files from your Win98 CD. Next, a System Settings Change menu will request that you restart your computer. Click Yes to restart the system.

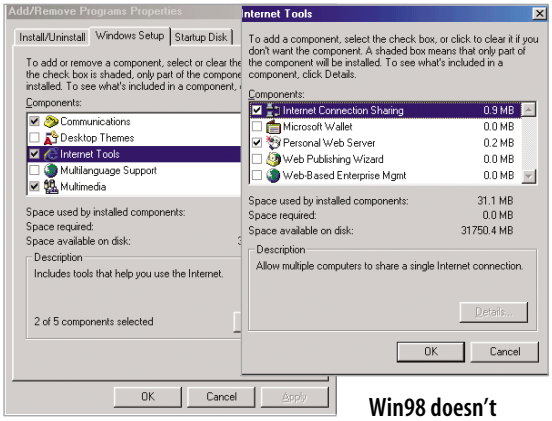
Share & Share Alike

Once you enable file and printer sharing, you'll need to choose which folders and printers you'd like to share over the network. Keep in mind that a shared folder also shares all of its subfolders; consider all of the files that will be shared before you share a folder. The good news is that you can share any folder: If you don't want to share your entire My Documents folder, you can share one of its sub folders, such as My Pictures.

Share folders. Open My Computer and then navigate to the folder you'd like to share. Don't open this folder; instead, right-click the folder icon and then select Sharing from the menu. When the folder's Properties menu appears, click the Sharing tab and then click the Shared As radio button. This button enables several options that appear on the same tab. The first option is Share Name: This is the name that will appear under your folder's icon on the network. By default, the folder's original name appears (for example, if you share your My Pictures folder, its share name remains My Pictures unless you change it). You can avoid some confusion by leaving the share name alone. This section also has a Comment field that lets you add a short description of the folder's contents. You can leave this field empty.

The Sharing tab also offers some advanced protection options. You can let other users view your files without letting them edit the files by clicking the Read-Only button. If you don't enter a password in the Read-Only Password field, any user can view the files.

The Full option is just that: full access. Network users can open files in this folder and edit them. You can enter a password to prevent certain users from accessing the files at all. The Depends On Password button lets you create separate passwords for Read-Only and Full access, which is a handy feature, as you may want to give Read-Only access to some users and Full access to others. Once you've filled these fields, click OK. The Properties window will close and your folder's icon will now have a picture of a hand that holds the folder.


Add/Remove Programs Properties
Install/Uninstall
Windows Setup
Startup Disk
To add or remove a component, select or clear the check box is shaded, only part of the compone installed. To see what's included in a component,
Components:
Communications
Desktop Themes
Internet Tools
Multilanguage Support
Multimedia
Space used by installed components:
Space required:
Space available on disk:
Description
Includes tools that help you use the Internet.
2 of 5 components selected
OK
Cancel
Apply
Internet Tools
To add a component, select the check box, or click to clear it if you don't want the component. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details.
Components:
Internet Connection Sharing 0.9 MB
Microsoft Wallet 0.0 MB
Personal Web Server 0.2 MB
Web Publishing Wizard 0.0 MB
Web-Based Enterprise Mgmt 0.0 MB
Space used by installed components: 31.1 MB
Space required: 0.0 MB
Space available on disk: 31750.4 MB
Description
Allow multiple computers to share a single Internet connection.
Details...
OK
Cancel

Win98 doesn't include the Internet Connection Sharing wizard by default. If you'd like to share your dial-up network connection, you'll need to install this feature from your Win98 installation CD.

Share Printers. You can let other network users send print jobs to your PC's printer. Make sure your printer is completely installed (attach your printer and then install the printer's drivers), then click Start, Settings, Printers. Locate the printer you'd like to share, right-click it, and then select Sharing from the menu. When the printer's Properties menu appears, click the Shared As radio button. The Share Name field contains the printer name that other network users will see when they look for your printer. As with folders, you can also enter a comment that further describes the printer. If you leave the Password field blank, any user on your network can access your printer. Enter a password and then share that password with approved network users to limit its access to them.

Network Neighborhood

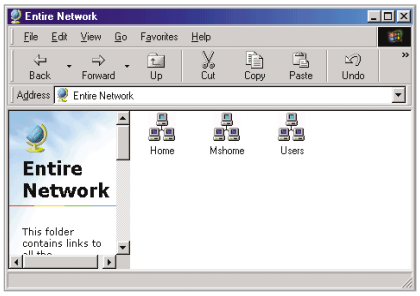
To find other PCs on your network, double-click the Network Neighborhood on your Desktop. Double-click Entire Network and then open your network's workgroup. You'll find both folders and printers here.

Set Up Your Internet Connection

If your PC has a dial-up modem or an Ethernet network card that is connected to the Internet via a broadband Internet connection, you can set up your Internet connection via Win98's built-in Internet Connection Wizard. If you installed Win98, you'll find a shortcut to this wizard on your Desktop. If you bought a used PC, you may find that the owner removed this icon. If the Desktop doesn't have an Internet Connection Wizard icon, click Start, Programs, Accessories, Internet Tools, and Internet Connection Wizard.

The wizard's first page lets you specify your Internet connection type. If you have a dial-up modem, indicate whether you already have an Internet service or whether you plan to sign up for one. If your PC uses a cable or DSL modem, click the radio button next to I Want To Set Up My Internet Connection Manually, Or I Want To Connect Through A Local Area Network (LAN). Click Next. IF you have a broadband connection, indicate that again at this page by clicking the appropriate radio button. Click Next again and then check the Automatic Discovery Of Proxy Server (Recommended) box.

When the Set Up Your Internet Mail Account page appears, click the No radio button (you can start your email program's setup at any time by double-clicking the program's icon) and then click the Next button. Check the To Connect To The Internet Immediately, Select This Box And Then Click Finish box. When you click finish, your default Internet browser (Internet Explorer, unless you've already installed a different browser) will open and display the default Web page.



Use the Network Neighborhood to browse your network. Once you find the appropriate workgroup, you can enter the group and then access its computers.

Use Windows 98SE's ICS wizard

Windows 98SE didn't introduce many major changes to Win98. In fact, Windows Millennium Edition didn't represent a major overhaul of Win98 either (home Windows users didn't get to experience a truly significant upgrade until Windows XP launched). But the second edition of Win98 did hail a few interesting features, including the Internet Connection Sharing wizard. This wizard automatically configures your PC to share your dial-up Internet connection with any other PC's networked to your primary computer. Be sure to run The Internet Connection Wizard prior to running ICS (Internet Connection Sharing), as ICS requires that your PC already have a working dial-up Internet connection.

Although you can download some of Win98SE's features for your Win98 PC, you won't be able to download ICS. You'll need to upgrade to Win98SE or buy the full version of Win98SE and install it on your Win98 PC (note that this clean install completely erases all data on your computer, including any documents, music files, or pictures).

Win98SE doesn't enable ICS by default, so you'll need to add it after you complete your Win98SE installation. To enable ICS, put your Win98SE disk into your CD drive. Next, click Start, Settings, Control Panel. Double-click the Add/Remove Programs icon and then click the Windows Setup tab when the Add/Remove Programs Properties window appears. The Components area displays several Windows components, including Internet Tools. Select Internet Tools and click the Details button. When the Internet Tools menu appears, check the Internet Connection Sharing box and click OK. Click the Apply button.

Windows opens the Internet Connection Sharing Wizard as soon as the installation completes and walks you through the steps to share your dial-up Internet connection.

Protect Your Network

Although Microsoft no longer supports Win98, you can still download updates that plug security holes in Win98. Be sure to install these updates on all of your Win98 PCs. To start the update process, click Start, Windows Update. Also, you should install antivirus software on all your PCs. You can learn more in this issue's Security section, starting on page 106. RS

BY JOSHUA GULICK

Windows Me Networking Wizards & Settings

Use Windows Me To Create Your Home Network

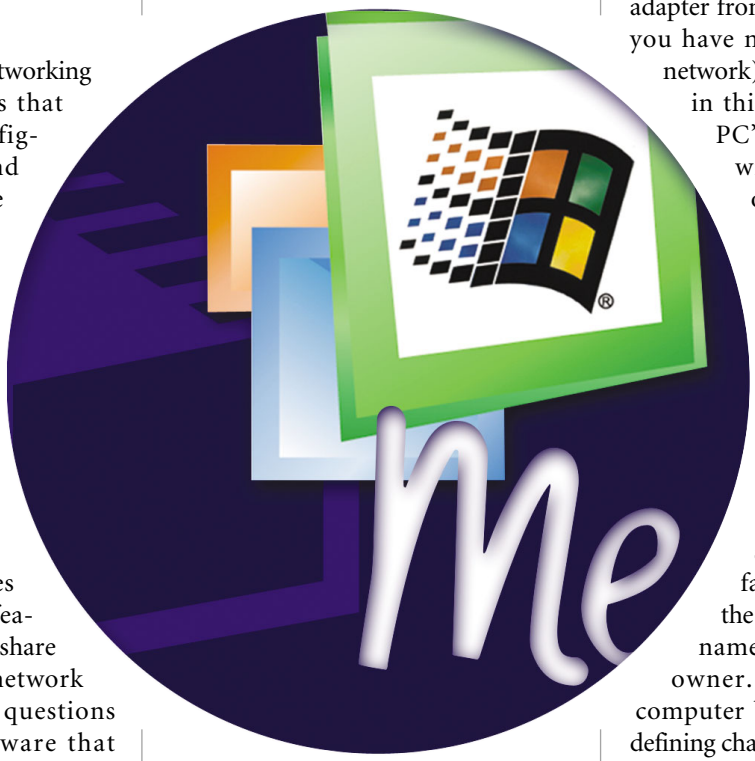
Although Windows Me is getting a little long in the tooth (Microsoft stopped offering support for Windows 98/Me in July 2006), you can still use the operating system's tools to connect your older computer to your home network. In fact, if you don't have any OSes newer than WinMe, you can use its networking tools to create your network and configure your older (Windows 95/98) machines. We'll show you how to take care of some of its most important networking tools and give you some tips for manually sharing folders and printers over your network.

Home Networking Wizard

Thanks to the Home Networking Wizard (a series of pages that offers step-by-step configuration instructions and options), you can configure your computer for your network in minutes. To find the icon, click Start, Programs, Accessories, Communications, Home Networking Wizard. You will only need to run the wizard once on each network computer.

The Home Networking Wizard opens with a welcome page that introduces the wizard's networking features (such as the ability to share your printer with other network computers). If you have questions about the types of hardware that make up a network, click the Using Home Networking link, which opens WinMe's Help And Support file. The link takes you directly to Help And Support's Home Networking section, which has basic instructions for choosing networking components and assembling your network. Because you've already assembled your network (presumably), you can skip the Using Home Network link and instead click the Home Networking Wizard's Next button.

The Internet Connection page is the first page that lets you adjust your PC's network settings. Here you'll need to indicate the method your computer uses to connect to the Internet. If you don't subscribe to an ISP (Internet service provider), simply click the No, This Computer Does Not Use The Internet radio button. If your computer connects directly to a system that has an Internet connection, select the A Connection To Another Computer On My Home Network That Provides Direct Access To My Internet Service Provider (ISP) option. Chances are, your network already has an Internet connection via your network router. If that's the case, select the A Direct Connection To My ISP Using The Following Device radio button and then choose your Ethernet adapter from the drop-down menu. If you have multiple LAN (local-area network) adapters, they will appear in this menu. Otherwise, your PC's only Ethernet adapter will already appear as the only option in the drop-down menu.

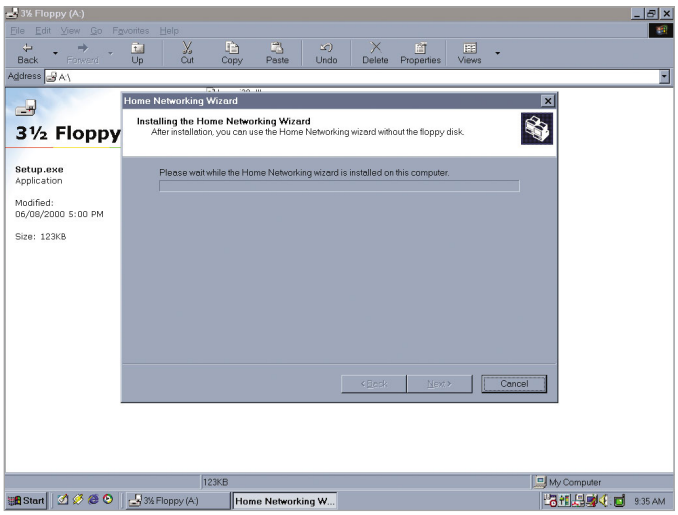


You'll need to choose a name for your computer when you reach the next page of the Home Networking Wizard (Computer And Workgroup Names). This name will identify your computer on your home network. If several people in your family have computers on the network, you may want to name each computer after its owner. You can also name the computer by its room or any other defining characteristic.

The page also lets you enter your workgroup name. If you used another computer to set up your network, you have probably already chosen a workgroup name. The name places all of your computers into a single group that can see each other and share files, so make sure that you enter the same workgroup name that the other computers on your network have. If you are using this PC to set up your network, write down your workgroup name after you've chosen it in case you need to manually configure other PCs later. (You probably won't need to manually configure your other PCs, as this wizard lets you create a setup disk that automatically adjusts this and other settings on your other PCs).

To enter your network's workgroup name, simply click the Use This Workgroup Name radio button and then enter the name. If you prefer not to make up a name, you can select the Use The Default Workgroup Name MSHOME (Recommended). That said, we recommend choosing a name that you can easily identify when you look for computers on your network later.

Next, you'll see the Share Files And Printers page. The Home Networking Wizard lets you share only your My Documents folder. This option shares all of the folders and files in your My Documents folder on the network. Don't worry if you want to share only certain folders within the My Documents folder: You can manually configure any individual folder to share files later (we'll show you how to share other folders later in this article). If you want to share your My Documents folder, click the appropriate checkbox. Once you click the My Documents Folder And All Folders In It checkbox, the Password button becomes active. If you want all PCs on your network to have easy access to your folders, you can ignore this button. (Note that when you click the Next button, a message will appear to warn you that you haven't password-protected the folders. Click OK to close this window and then click the Next button again.) If you choose to protect the folders, click Password, enter a password, and then click OK. Finally, give this password to the other network users with whom you'd like to share access.



If you don't see an Ethernet adapter listed here, check your motherboard's I/O (input/output) ports at the back of the PC to make sure the motherboard has a built-in Ethernet port.

You can also share your printers via this page. Any printers attached to your computer will appear on the page; simply click the checkboxes next to the printers you wish to share. Keep in mind that other network computers can access these printers only when this computer is powered on. If you shut down this computer regularly, consider moving the printers to a computer that is always on.

Once you click the Next button, the Home Networking Setup Disk page will appear. The Home Networking Setup disk lets you install the wizard on Win95/98 computers so you can easily configure those computers. If you are simply adding this computer to an existing network, you can skip this step (after all, you're not going to configure any other computers). If this is the first computer you configure for your home network, take advantage of this feature. Click the Yes, Create A Home Networking Setup Disk radio button and then click the Next button.

The next page requests a floppy diskette. Insert a blank diskette (if it isn't blank, the feature will erase any files on the diskette before adding the Home Networking Setup Disk files) and click the Next button. The wizard will install the files and display Completing The Home Networking Wizard. Remove the diskette and click Finish. Click Yes when asked to restart the PC.

Share Folders & Printers

WinMe includes a special networking menu that lets you easily see all of the shared folders on your network: My Network Places. In this window, many network folders and printers appear as icons, which means you can open any (shared) folder from another PC as though it were another folder on your PC. (If you don't see the network folders, you can easily find them by clicking the Entire Network icon in My Network Places.) The My Network Places icon may appear on your Desktop when you first install WinMe. It will also appear once you've set up your network via the wizard.

Double-click the My Network Places icon. Now that you've run the Home Networking Wizard, you'll see the folders that you shared during the wizard. If you don't see other PCs' shared folders in this window, double-click the Entire Network icon and then navigate to the appropriate PC name. When you open that PC, you'll see its shared folders and printers.

To share additional folders, you'll need to configure them manually. Minimize or close this window and

open My Computer. Open your hard drive and choose the folder you'd like to share. Right-click the folder and click Sharing. When the folder's Properties window appears, select the Shared As radio button and enter a name that describes the folder on the network. (By default, the folder's name appears.) You can also add a description in the Comment field. The comment will only appear when a user selects that folder's icon (it appears on the left side of the window).

Next, you'll choose the folder's Access Type. The Read-Only setting allows users to view the folder's contents, but won't allow users to change the files. You can set a password for Read-Only access. If you choose the Full setting, users can both access and make changes to the folder's contents. You can also set a password for this option. If you want to allow Full access to some users and Read-Only access to others, choose Depends On The Password and enter different passwords in each Passwords field. Be sure to enter different passwords, as identical passwords will let some users obtain access you didn't intend them to have.

You probably shared your printer when you ran the Home Networking Wizard. If you didn't, or if you'd like to share a different printer from your PC, click Start, Settings, then Printers. Right-click the printer you'd like to share and click Sharing. When the printer's Properties menu appears, click the Sharing tab and click the Shared As radio button. Name your printer in the Share Name field. You can also enter a comment. If you'd like to control who uses the printer, enter a password in the Password field.

Internet Connection Wizard

To access the Internet through your home network, you'll need to run the Internet Connection Wizard. By default, Windows places a Connect To The Internet icon on your Desktop. If your PC doesn't have this icon, start the wizard by clicking Start, Programs, Accessories, Communications, Internet Connection Wizard.

When the wizard's main page appears, click the radio button next to I Want To Set Up My Internet Connection Manually, Or I Want To Connect Through A Local Area Network (LAN). Click Next. When the Setting Up Your Internet Connection page appears, click the I Connect Through A Local Area Network (LAN) radio button and then click Next.

At the Local Area Network Internet Configuration page, check the Automatic Discovery Of Proxy Server (Recommended) box. The next page asks whether you'd like to set up your email account. If you'd like to set up your email account settings now, click the Yes radio button. Otherwise, click No and then click Next. Click Finish.

Dial-Up Networking

Dial-Up Networking lets you connect to a remote computer or network via the Internet. You'll need a dial-up modem and a dial-up Internet service subscription to use this feature. To start WinMe's Dial-Up Networking Wizard, click Start, Programs, Accessories, Communications, Dial-Up Networking and then double-click the Make New Connection icon. When the Welcome To Dial-Up Networking window appears, click the Next button. The Install New Modem will appear. Click Next to let it search for your modem. Once this mini-wizard completes, return to the Dial-Up Networking Wizard and follow the wizard's instructions to complete your connection.

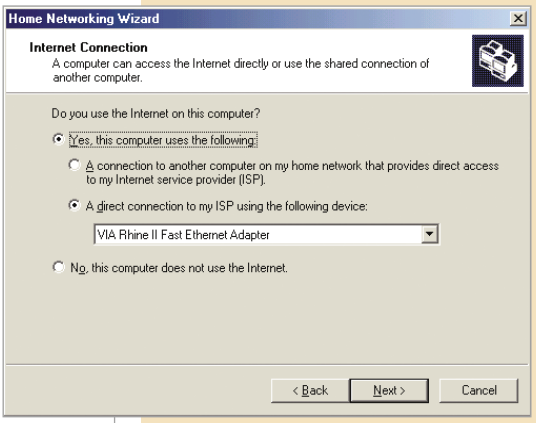
Protect Your Network

Now that you've finished setting up your network, make sure your PCs have adequate protection against malware. To that end, be sure to install all of Microsoft's Windows Updates (connect to the Internet and click Start and Windows Update). You should also install an antivirus program. You can learn more about antivirus protection in the Security & Privacy section starting on page 106. Finally, change your shared folders' passwords from time to time to prevent malicious users from stumbling across an old password. RS

BY JOSHUA GULICK

Use The Home Network Setup Disk

Windows Me's Home Network Setup floppy diskette lets you quickly configure your Win95/98 computers via the same easy-to-use networking wizard that you used when configuring your WinMe PC. To run the Home Network Setup disk's wizard on your Win95/98 computer, pop the floppy diskette into the PC, open My Computer, open the floppy diskette drive, and then double-click the Setup.exe file. When the wizard begins, it will display a window you haven't seen before: Installing The Home Networking Wizard. Once the wizard finishes installing to your computer, it will display the same pages as the wizard on your WinMe PC.


Home Networking Wizard
Internet Connection
A computer can access the Internet directly or use the shared connection of another computer.
Do you use the Internet on this computer?
Yes, this computer uses the following:
A connection to another computer on my home network that provides direct access to my Internet service provider (ISP).
A direct connection to my ISP using the following device:
VIA Rhine II Fast Ethernet Adapter
No, this computer does not use the Internet.
< Back
Next >
Cancel

WinMe's Home Networking Wizard setup disk lets you use the wizard on PCs that run Win95/98.

Windows 2000 Networking Wizards & Settings

Go Ahead & Get Connected

Almost every version of Windows includes a networking wizard to make it easier for users to connect to the Internet or to another computer. Of course, each network wizard has its own peculiarities that you need to know about. In this article, we'll explore the Windows 2000 Networking Wizard.

Start The Wizard

First, we need to discuss Win2000 networking. In most cases, Win2000 will automatically configure network interfaces (such as your Ethernet card). If you have a broadband connection, there's a good chance Win2000 will automatically configure it for you for Internet access. Before you try using the Network Connection Wizard, try opening a browser and see if you can connect to the Web. The options below pertain primarily to networking via modems, serial, and parallel cables.

We'll start by clicking Start, selecting Settings, and clicking Control Panel. In the Control Panel, double-click Networking And Dial-Up Options and then double-click Make New Connection.

If you haven't provided Windows with your country and area code, the Location Information window will appear. Enter your area code in the specified field and enter any dialing prefix you may need to get an outside line (this usually only applies in an office setting). If you're not sure whether you have tone or pulse dialing, leave Tone Dialing selected. When you click OK, the Phone And Modem Options window will appear. Click OK to close this window and get to the wizard.

To begin the wizard, click Next. You'll then see five options provided by the wizard: Dial-Up To Private Network, Dial-Up To Internet, Connect To A Private Network Through The Internet, Accept Incoming Connections, and Connect Directly To Another Computer.

The first option, Dial-Up To Private Network, lets you configure Win2000 to connect to a remote computer via a modem. Technically you can use this option to connect to the Internet, but it's best to use the second option, Dial-Up To Internet, for that purpose. If you need to modify the default settings used for your broadband connection, select this second option as well. The third option, Connect To A Private Network Through The Internet, allows you to connect to a remote computer via the Internet. This option varies from the first option in that you don't dial directly into the private network, but connect to the Internet first and then connect to the private network. If you want to allow others to connect to your PC,

whether it's over the Internet or directly through a modem, you should select the fourth option: Accept Incoming Connections. Finally, the last option, Connect Directly To Another Computer, allows you to use either a serial or parallel cable to connect two computers.

Dial Up To A Private Network

If you want to dial into a private network, select the first option and click Next. Begin by entering the phone number you want to dial. If you're connecting to a computer in another area code or another country, place a check in the Use Dialing Rules checkbox. Enter the area code for the computer you're connecting to in the Area Code field. If you need to change the Country/Region, click the drop-down list and select the proper entry. If the computer you're dialing is in the same area code, be sure to remove the check in the Use Dialing Rules checkbox. Click Next to continue.

If other people have their own Win2000 accounts and you don't want them to have access to the connection you're creating, select Only For Myself and click Next. If you want all users on the system to have access to the connection, select All Users and click Next. Provide a name for the connection. This can be anything but should probably be something descriptive of the connection. Click Finish to finish the connection. You should see an entry for the new connection appear in the Networking And Dial-Up Options window.

Dial Up To The Internet

Of all the options, this is the most complicated. Selecting this option starts the Internet Connection Wizard, which is slightly different from the Networking Wizard.

The Internet Connection Wizard begins with three options: I Want To Sign Up For A New Internet Account, I Want To Transfer My Existing Internet Account To This Computer, and I Want To Set Up My Internet Connection Manually, Or I Want To Connect Through A Local Area Network. The first option allows you to sign up for Internet service through one of Microsoft's partners. The second allows you to automatically configure your computer to connect to an existing service provider. The final option lets you manually specify your Internet connection settings. Note that the first two options require your modem to be on and connected to an active phone line.

The first two options are fairly self-explanatory. The third option is the most complicated and the most often used. Start by telling Windows how you connect to the Internet. If you connect through a modem, click I Connect Through A Phone Line And A Modem and click Next. If you have a broadband connection, select I Connect Through A LAN (Local-Area Network) and click Next.

Modem Connections. If you have a dial-up Internet connection, Windows may need to install the hardware drivers for your modem if you haven't installed them already. Windows will try to detect your modem and automatically install the proper driver (make sure your modem is on and properly connected to the PC). If Win2000 can't detect your modem, you may have to select it from a list or install the driver manually from the CD that was included with the modem. After configuring the modem, you'll need to specify a number to dial. Your ISP (Internet Service provider) should provide you with the proper dial-in number. Normally, this number will be a local number. If you need to adjust the area code, however, place a check next to Use Area Code And Dialing Rules and enter the proper area code.

Below the dialing options is an Advanced button that opens a separate Advanced Options window. In most instances, you shouldn't have to adjust your settings. If you connect to the Internet using a protocol other than PPP (Point-to-Point Protocol) or need to use a logon script or specify a static IP (Internet Protocol) address or DNS (Domain Name Service) server, click the Advanced button. Usually, the default settings will work fine.

If you click the Advanced button, you can select whether to use PPP, SLIP (Serial Line Internet Protocol), or C-SLIP (Compressed SLIP) to connect to the Internet. You can also specify a logon procedure (options include None, Logon Manually, and Use Logon Script). Click the Address tab at the top of the window if your provider assigned your computer a static IP address or if you need to manually specify your ISP's DNS servers. You should be able to get this information from your ISP, but in most instances you can leave the default values in place. Click OK to close the Advanced Options box.

Network Connection Wizard
Welcome to the Network Connection Wizard
Using this wizard you can create a connection to other computers and networks, enabling applications such as e-mail, Web browsing, file sharing, and printing.
To continue, click Next.
< Back
Next >
Cancel

The Network Connection Wizard is the primary networking wizard in Windows 2000. Select the proper option and click Next.

Click Next and provide a Username and Password in the proper fields. Again, if you don't have this information, you can get it from your ISP. Click Next, provide a name for the connection, and click Next.

Whenever you configure an Internet connection, Windows will give you the option of configuring an email account in Outlook Express. If you plan to use an email client other than Outlook Express (such as Thunderbird

or Eudora), select No and click Next. Click Finish to finish creating the connection. If you do want to create an email account in Outlook Express, click Yes and follow the instructions.

Broadband. Although Win2000 will usually configure a broadband Internet connection for you, there may be some cases in which you need adjust the default settings. Select I Connect Through A Local Area Network (LAN) and click Next.

In most cases, you can simply leave Automatic Discovery Of Proxy Server checked and then click Next. If you know your proxy server's settings (the hostname or IP address of your proxy server as well as the port number you use to connect to it), you can check Manual Proxy Server and then click Next. In most cases, you can enter the hostname and/or IP address and port number for your proxy server in the field next to HTTP and check the Use The Same Proxy Server For All Protocols. Otherwise, you'll need to enter a proxy server next to each data type and click Next.

After clicking Next, Win2000 will offer to create an email account for you in Outlook Express. If you click Yes, the operating system will walk you through configuring your email account.

Connect To A Private Network Through The Internet

This option is very straightforward. Start by providing the hostname or IP address of the computer you want to connect to. A hostname might be www.smartcomputing.com, while an IP address consists of four sets of numbers between 0 and 255, with each number separated by a period (e.g., 192.168.123.254). You'll need to provide this information in order to connect to a computer on the Internet. Click Next and then select whether the connection should be available for everyone or only for yourself. Click Next, enter a connection name, and click Finish.

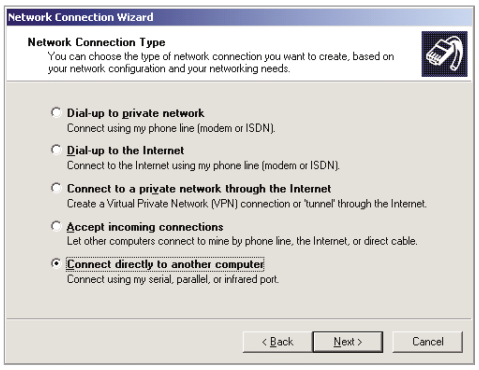
Accept Incoming Connections

You can make it possible for others to connect to your PC. These remote users can connect over the Internet, a modem, or one of your computer's connection ports (such as a parallel port, for instance). You can limit who has access to the PC and how they access it. If you want others to connect to your PC using a modem, parallel, or serial port, select the device from the list. If you just want to accept incoming connections from the Internet, don't select any additional devices and click Next. If your PC has a static IP address (normally, you have to pay extra for this option), you can select Allow Virtual Private Connections for added security. If, however, you don't have a static IP address for your PC, you'll need to select Do Not Allow Virtual Private Connections. Click Next to view a list of user accounts on the system. Place a check next to any account that you want to make available online. You also can click the Add button to create a new account (you'll need to provide a username, full name, and password for the account). Click Next to continue.

Finally, select what network components users have access to. For instance, if you don't want users who connect over the Internet to have access to File And Printer Sharing For Microsoft Networks, be sure to clear the checkbox next to that item. You can also add components by clicking the Install button (you may need your Win2000 installation disc). Click Next, provide a name for the connection, and click Finish.

Connect Directly To Another Computer

This option is for configuring alternative connections between two PCs. Select this option if you need to configure a connection between two PCs over a serial port or parallel port. After selecting Connect Directly To Another Computer, you'll need to select whether you want to configure the computer as a host or a guest. If you have documents and other files on the computer that you want to share with other computers, select Host. If there are files on the other computer that you want to be able to access, select Guest.


Network Connection Wizard
Network Connection Type
You can choose the type of network connection you want to create, based on your network configuration and your networking needs.
Dial-up to private network
Connect using my phone line (modem or ISDN).
Dial-up to the Internet
Connect to the Internet using my phone line (modem or ISDN).
Connect to a private network through the Internet
Create a Virtual Private Network (VPN) connection or "tunnel" through the Internet.
Accept incoming connections
Let other computers connect to mine by phone line, the Internet, or direct cable.
Connect directly to another computer
Connect using my serial, parallel, or infrared port.
< Back
Next >
Cancel

The Connect Directly To Another Computer option lets you connect to your Windows 2000 system from another computer using a serial or parallel port.

Whether you decide to configure the computer as a guest or a host, the next step is the same. Select the device you want for incoming or outgoing connections and click Next. If you're configuring the computer as a host, select which accounts you can sign on to from the other computer. If you're configuring the computer as a guest, choose whether the connection should be available for all users or just for you and click Next. The final step, regardless if you're configuring a host or a guest connection, is to provide a name for the connection and click Finish.

As you've probably noticed, the most complicated thing about the Network Connection Wizard is understanding what it can and cannot do. If you want to configure a home network, for instance, the Network Connection Wizard isn't the right place to look. On the other hand, it works well if you need to configure alternative types of connections, especially connections over a modem, serial cable, or parallel cable. RS

BY CHAD DENTON

Sit, Sip & Surf

Connect Anywhere With Wi-Fi Internet

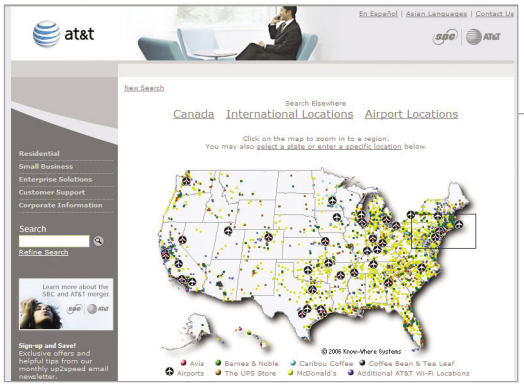
Visit any local coffee shop and check out the faces of the laptop patrons. They seem so happy and efficient, but the gourmet coffee isn't a laptop customer's only buzz. High-speed wireless Internet access makes it great to surf and work wherever you please. However, before you sprint outside with your laptop, you should know that you'll need more than just your laptop's wireless card to receive Internet access. You'll have to find a **hotspot** to access wireless Internet outside your home network. A hotspot is a specific geographic location such as a coffee shop or airport lobby that offers wireless Internet access. Such places may offer hotspots for free or a fee and each method presents distinct advantages and disadvantages.

You may already know a number of free hotspots near you, but that doesn't guarantee you'll be able to find free hotspots on the road. A wireless Internet service provider offers access to thousands of hotspots, but you'll need to log on at a specific service provider's hotspot to access the Internet. A service provider's roaming agreement will give you more complete coverage, but roaming charges will take more from your pocket book. Choosing the right plan of attack for you means doing a little research.

Splash Into A Hotspot

You can sit, sip, and surf at some hotspots for free, but access at a location such as Starbucks requires a WISP (Wireless Internet Service Provider) such as T-Mobile. A hotspot will have a WLAN (Wireless Local-Area Network) that you will need to access to surf the Internet. Use your wireless card to search for the WLAN and pick a network to connect to the Internet. If access to the network is not free, when you open a Web browser you will see payment options on a "splash page." A splash page is a Web page that allows you to sign in to a hotspot's WISP. The splash page may also indicate a list of supported roaming Wi-Fi providers. A Wi-Fi provider such as Boingo (www.boingo.com) is a WISP **network aggregator**, a service provider that offers access points from at an assortment of other providers' hotspots. Boingo provides one large roaming network of 7,000 hotspots, and charges a flat fee of $21.95 a month for access to select hotspots from more than 100 service providers. A network aggregator's collection of service providers gives you Internet access at a variety of different businesses and chains. You can also find a wide variety through a large provider, such as T-Mobile (www.t-mobile.com), that offers Wi-Fi services at Starbucks, Borders, FedEx Kinko's, Hyatt Hotels, and the airline clubs of American, Delta, United, and US Airways for $29.99 a month.

T-Mobile, Wayport (www.wayport.com), and Boingo are just a few hotspot providers that deliver wireless access at thousands of hotspots, but a large service provider may not be the right provider for the places you visit. To find the service provider who offers the most access points in your area, search a hotspot online directory such as JiWire (www.jiwire.com), WiFinder (www.wifinder.com), or Wi-FiHotSpotList.com (www.wi-fihotspotlist.com). To use JiWire, enter your address into a directory and



Wi-Fi hotspots are just blips on the map compared to cell phone coverage areas.

narrow your search by free hotspots, a specific provider, or all providers. JiWire lists the names, addresses, and proximity of the hotspots within your chosen range. Click a link to a service provider's Web site and you can find a list or map of all the available hotspots from that WISP. Use an online directory such as Wi-Fi-FreeSpot (www.wififreespot.com) or Ilovefree-WiFi (www.ilovefreewifi.com) to locate free hotspots. You won't have to weed out the pay services. Establishments that typically offer free Wi-Fi include independent coffee shops, restaurants, airports, and lodging chains. Panera Bread is a national café chain that has more than 760 free hotspot cafes in the United States. Visit http://www.panerabread.com/locations.aspx?WiFi=1 to find a location near you.

The Dilemma

It's hard to justify paying for Wi-Fi access when you can find free hotspots, but the bottom line is that travelers cannot rely on free hotspots to be at convenient locations. A traveler who hops from airport to airport will find variations of Wi-Fi service providers, free hotspots, and wired-only Internet access. Business people on the road need to find a balance between a provider that covers the locations they visit, a provider with a large coverage area, and a price that they can afford.

A good way to select a provider is to choose a service based on the businesses or locations where you plan to access Wi-Fi most often. We searched Wi-FiHot-SpotList.com to find which hotspot WISPs are available at businesses in Boston. Several Boston hotels used Boingo, including a Best Western, Boston Marriott, Four Seasons, and Embassy Suites. Boingo hotspots were also available at two Barnes & Noble bookstores and four Rebecca's Café locations. T-Mobile provided hotspots at American Airlines clubs and lounges, two Borders, six FedEx Kinko's, and 20 Boston Starbucks locations. A particular chain will often use the same provider nationwide, which should influence your decision if you visit one often. McDonalds and Wayport offer Wi-Fi at over 7,000 McDonalds across the country. You're ready to surf at any McDonalds that offers Wi-FI if you have a Wayport membership, or you can charge a one-time connection that costs $2.95 for 2 hours of service to your credit card if you don't have a service provider.

Short Timers

If you only access wireless hotspots a few days a month, then you don't need a year-long plan. Infrequent hotspot seekers can either search for free hotspots or utilize a one-day pass, which usually costs around $10 a day. T-Mobile offers a HotSpot 24-hour DayPass for $9.99 or Pay As You Go service starting at $6 per login for 60 minutes and 10 cents per minute thereafter. Boingo As-You-Go provides 24 hours of connection time at one location for $9.95. Through Wayport, you can purchase three connections for $25, eight connections for $50, or 20 connections for $100. Each connection gives you unlimited access in one location for that day. A single-use pass won't get you trapped into a long term contract and you'll be able to use the service when you need it. Of course, the shorter the plan, the more you'll end up paying per hour.

Get More Than You Pay For

With a little time and patience you will probably be able to find a free hotspot close to you. Check out local coffee shops, restaurants, libraries, and hotels to see if you can get online for free. Use a hotspot finder tool such as the IOGEAR Wireless Hot-Spot Finder to search for Wi-Fi while you walk down the street. The Hot-Spot Finder has a range of 500 feet and uses 4 LEDs to display signal strength. You don't even need your laptop or PDA with you to find a signal. A wireless signal finder fits on your keychain.

Unwired Future

Philadelphia, San Francisco, and Minneapolis have all announced plans to make each of their cities one large wireless hotspot or **mesh network**. Wireless Philadelphia's Business Plan pronounces, "Wireless Philadelphia intends to create a digital infrastructure for open-air Internet access and to help citizens, businesses, schools, and community organizations make effective use of wireless technology to achieve their goals." Some small cities such as Chaska, Minnesota already employ a citywide mesh network. The city of Chaska charges residents $16.99 a month for unlimited wireless access for three computer accounts.

Most cities are taking a wait-and-see attitude toward wireless mesh networks. In the future, Wi-Fi hotspots may become mesh networks and should resemble the current cell phone coverage area. As more hotspots create larger coverage areas, you'll have more opportunities to connect from just about anywhere. But until the coverage area grows, you'll need to pick a service provider or use free hotspots at limited locations. RS

BY NATHAN LAKE

Configure Your Notebook For Access On The Road

Get Wireless Internet Wherever You Go

According to Ipsos Insight's annual *The Face of the Web* study, Americans spent an average of 11.4 hours online each week in 2005. For many of us who work at a computer all day, that number is probably even higher. Given the chunk of time we devote to online activities and the number of things we use the Internet for, it's no wonder wireless Internet access is becoming increasingly available.

With today's technology, we have more ways to connect to the Internet than ever before. You can connect via a wired connection at home, at the office, or at school. You can also surf the Web on your cellular phone or through a wireless card built into your laptop computer when a hotspot is available. One of the newest ways to connect to the Internet on your laptop is to create a hotspot for yourself using a cellular Internet connection from your cell phone or special PC modem card.

Given the various connection options available, it can be tough to decipher which method is best for you. To help, we've compiled information on three leading options for wireless Internet access: Wi-Fi, EVDO (Evolution Data Optimized), and EDGE (Enhanced Data for GSM Evolution). We'll look at the benefits and detriments of all of the options, consider the cost of each option, and explain the basics of creating a connection using each of the three methods.

Wi-Fi

Wi-Fi is another name for the IEEE (Institute of Electrical and Electronics Engineers) 802.11 standard. This standard makes it possible for users with Wi-Fi products to use them with other Wi-Fi hardware, regardless of brands. Put another way, Wi-Fi is a standard that wireless hardware uses to communicate with other hardware in order to connect to a network. Many versions of Wi-Fi comprise wireless networking, including 802.11a, 802 .11b, 802.11g, and 802.11n. Although the Wi-Fi standards enable communication among wireless hardware, not all hardware is compatible with all versions of Wi-Fi.

Although Wi-Fi technically describes the technological standard behind a wireless network, many people use the term to describe wireless Internet made possible by connecting to a hotspot. You may have seen signs for hotels that use the term in this way by advertising "Free Wi-Fi".

In order to connect to an existing Wi-Fi network, you'll need a wireless network card. You can buy these cards in three forms: as an internal card for your desktop PC, as a removable PC card for your laptop, or as an external USB device. If you've purchased a laptop within the past few years, you may not need to purchase anything, as many new laptops have integrated wireless network cards.

Pros. With the right equipment, Wi-Fi lets you convert an existing wired network into a wireless one. This makes it easy to expand your network and make greater use of a wired connection. A wireless network can accept multiple simultaneous connections from different devices, including laptop and desktop PCs.

Wi-Fi is a common method of broadcasting Internet connections to various wireless devices. In many cases, it's more cost effective to set up and maintain a wireless network at home or in a small business such as a café than it is to wire a building with multiple connection points. A basic wireless network will include a wireless router, such as the Linksys Wireless-G Broadband Router WRT54G ($69.99; www.linksys.com) and desktop or notebook PC cards such as the Linksys Wireless-G PCI Adapter WMP54G ($59.99) or Linksys Wireless-G Notebook Adapter WPC54G ($59.99).

Wi-Fi networks are widely available at many travel destinations, including airports, hotels, restaurants, and coffee shops. Some connection points are free, whereas others charge a small fee to access the network. Additionally, Wi-Fi networks are relatively easy to connect to and require little setup,

which makes them ideal for even the casual PC operator. Once connected, you can surf the Internet, send and receive email, and download files.

Cons. Wi-Fi is limited in its broadcast range; you can only connect to a Wi-Fi network when you are within range of an access point or router. Although some 802.11b and 802.11g networks claim to support a range up to 150 feet indoors and 300 feet outdoors, walls, concrete, and other objects affect the actual range of wireless networks. In addition, even though Wi-Fi is available at many popular travel destinations, many places do not offer a connection for public access.

Security is also limited with Wi-Fi networks. Although you can lock down a private Wi-Fi network, such as one at your home, you cannot control the security of open Wi-Fi networks such as those you might access at a hotel or coffee shop. As a result, surfing the Web on some of these unsecured wireless networks can put you at a greater security risk. You can protect yourself with a firewall and other means, but this protection is somewhat limited.

Although a Wi-Fi network may give you a high-speed connection to a wireless network, your true connection speed to the Internet is limited by the bandwidth coming in to the network. If multiple people access a network at the same time, this can reduce the speed of transferring and receiving data from the Internet.

Get Connected. To connect to a Wi-Fi network in Windows XP, click Start, open the Control Panel, and then double-click Network Connections.

In the Network Connections menu, double-click the Wireless Network Connection icon. This will bring up a Wireless Network Connection dialog box that lets you view wireless networks within range of your PC. To retrieve a list of wireless networks, click Refresh Network List on the left. Once you see the network you want to connect to, click it, then click the Connect button. During connection setup, you can enter special settings for a network, including passwords and security keys that let you access secured networks.

Alternatively, you may wish to use a wizard to set up a wireless connection. To do so, click the Set Up A Wireless Network For A Home Or Small Office link in the left column of the Wireless Network Connection dialog box. Proceed by entering the appropriate information in the dialog boxes until you are finished with the wizard.

EVDO

In 1999, Qualcomm developed the initial design of EVDO in order to meet IMT-2000 (International Mobile Telecommunications-2000) requirements for a method of stationary communication that has a downlink speed greater than 2Mbps (megabits per second). The goal behind IMT-2000, and thus the goal of EVDO, was to create a standard for high-speed data transfer using cellular technology.

Wi-Fi adapters, such as the Linksys Wireless-G PCI Adapter WMP54G ($59.99; www.linksys.com), give your desktop PC the ability to connect to a Wi-Fi network.

Currently, EVDO standards are available in two forms: as Release 0 networks and as Revision A networks. EVDO Release 0 can send data to your EVDO-equipped device at speeds up to 2.4Mbps. Release 0 networks can upload data at up to 153Kbps (kilobits per second). The newer version of EVDO, Revision A, increases the maximum speed to 3.1Mbps on the forward link (downlink) and 1.8Mbps on the reverse (uplink) link. EVDO is only compatible with CDMA (Code Division Multiple Access) cellular carriers. The two most popular CDMA carriers in the United States are Sprint (www.sprint.com) and Verizon Wireless (www.verizonwireless.com).

Pros. One of the benefits of EVDO and other cellular technologies is the ability to roam seamlessly between connection points. An EVDO connection should keep you connected to the Internet even if you are traveling in a car. However, because EVDO service is not currently available in all locations throughout the United States, you may lose an EVDO connection while traveling or drop back to the slower 1xRTT (1 times Radio Transmission Technology) service, which is limited to 144Kbps.

EVDO is available for both mobile phones and laptops. Some smartphones, such as the Palm Treo 700p ($399.99 with a two-year contract; www.palm.com), come with built-in DUN (dial-up networking), which lets you use the EVDO connection on your phone as a modem for your laptop, thereby giving you high-speed Internet access on your notebook.

Another benefit to EVDO is its speed in comparison to previous technologies. Sprint claims that its Mobile Broadband service offers average wireless data speeds of 400 to 700Kbps with peak rates up to 2Mbps. Verizon claims its BroadbandAccess service offers average speeds of 400 to 700Kbps.

Because EVDO signals travel over cellular lines, EVDO provides the opportunity for areas without cable-modem or DSL (Digital Subscriber Line) high-speed Internet to receive Internet access. In some cases, this is the best way to provide broadband Internet access to these rural areas. Although most people do not find it cost effective to use an EVDO connection as a primary connection in

rural areas, it is a good option for travelers requiring an Internet connection wherever they go.

EVDO also provides data authentication and protection, which gives users the ability to securely access a corporate VPN (virtual private network) anywhere they can receive a cellular signal. Because EVDO isn't an open network like Wi-Fi, you're less susceptible to security breaches.

Cons. Probably one of the largest detriments to any type of cellular Internet connection is its cost. In fact, EVDO will generally add at least $60 to your monthly cellular bill. Verizon Wireless offers BroadbandAccess for $59.99 per month, with a two-year customer agreement and qualifying voice plan. Users who would prefer to connect their laptop directly to the Internet using BroadbandAccess will also need an EVDO PC card, which starts at $49.99 with a two-year agreement.

Sprint's Mobile Broadband EVDO service costs about the same as Verizon's BroadbandAccess. At press time, Sprint was offering unlimited Mobile Broadband service for $59.99 per month with a two-year wireless agreement, and a compatible PC card for $49.99 with similar qualifications.

Get Connected. To connect to an EVDO network, you'll need a compatible phone or PC card. With the phone or card in hand, install the software that will tell your notebook how to use the phone or PC card as a modem. The software will vary depending on the service provider and type of phone or card you are using, so follow the manufacturer's instructions for installation.

After the installation is complete, you should be able to connect your phone or plug the PC card in to your notebook, initialize the connection, and begin surfing the Internet. Depending on the software and security restrictions with your carrier, you may need to enter a user name and password in order to use your EVDO service on your laptop.

In some cases, using a cellular phone as a modem for your computer may disable the ability to place or receive calls on your phone. Be aware of this if you are expecting an important call.

EDGE

EDGE is the GSM (Global System for Mobile Communication) counterpart of EVDO. Like EVDO, EDGE uses cellular phone lines to access the Internet. As a result, the pros and cons, along with the steps required to connect to a network on your notebook, are very similar. The two primary GSM carriers in the United States are Cingular (www.cingular.com) and T-Mobile (www.t-mobile.com).

The Palm Treo 700p ($399 with a two-year contract; www.palm.com) lets you use the EVDO connection on your phone as a modem for your laptop.

Pros. Like EVDO, EDGE is available for both laptops and cellular phones. In the United States, Cingular offers BroadbandConnect, which uses HSDPA (High Speed Downlink Packet Access) technology, a step up from EDGE. HSDPA shares a common core network with GSM/EDGE, and is faster than GSM/EDGE. Cingular's BroadbandConnect is available in 52 communities and boasts average connection speeds between 400 and 700Kbps on the downlink and bursts to more than a megabit per second.

When a HSDPA connection is unavailable, your BroadbandConnect device will switch to an EDGE or GPRS (General Packet Radio Service) network if available. GPRS is slower than EDGE and has a transfer rate of 30 to 45Kbps. The Cingular EDGE network is available in more than 13,000 cities and towns along 40,000 miles of highways, providing average data speeds between 70 and 135Kbps.

T-Mobile also offers EDGE connectivity in the United States. T-Mobile's Total Internet plan differs from other carrier offerings in that it gives unlimited GPRS, EDGE, and Wi-Fi Internet connectivity in a single bundle. T-Mobile's GPRS network claims speeds up to 56Kbps, with EDGE rates up to three times faster than GPRS.

Cingular claims that its EDGE network is more secure than Wi-Fi because it utilizes SIM (subscriber identity module) cards and other encryption features. T-Mobile also uses SIM card-based network authentication and encrypted data transmission to secure data communications.

Cons. As mentioned for EVDO, one of the deterrents to wireless high speed Internet on a cell phone is cost. Although the price and choices for EDGE service may differ, the additional monthly fee for EDGE is cost-prohibitive for many people.

To connect to the Cingular BroadbandConnect service, users must purchase a PC card for $99.99 after rebate with a qualifying data plan. If you already have a voice plan and contract with Cingular that qualifies you for discounts, you can purchase an Unlimited Data Connect plan for $79.99 per month. Users who only need limited data access can purchase monthly plans starting at $19.99 for 5MB.

T-Mobile's Total Internet plan costs $49.99 per month, and requires a compatible cellular phone or PC notebook card. At press time, the Sony Ericsson GC89 PC notebook card from T-Mobile was selling for $149.99 with a qualifying rate plan and contract.

Although speeds vary, EDGE networks are generally slower than EVDO networks. When an HSDPA connection is available, you're likely to have speeds comparable to EVDO. With a standard EDGE connection, you're more likely to experience speeds in the range of 70 to 135Kbps. The lowest tier of GSM Internet connectivity, GPRS, is comparable to dial-up, about 56Kbps.

Begin Browsing

With a number of wireless Internet connectivity options available, it can be hard to decide which one will best suit your needs. When deciding, consider cost, availability, and connection speed. By considering all factors, you'll find the service that will give you the Internet connection you need to complete your online tasks. RS

BY JENNIFER JOHNSON

Wireless Internet Comparison

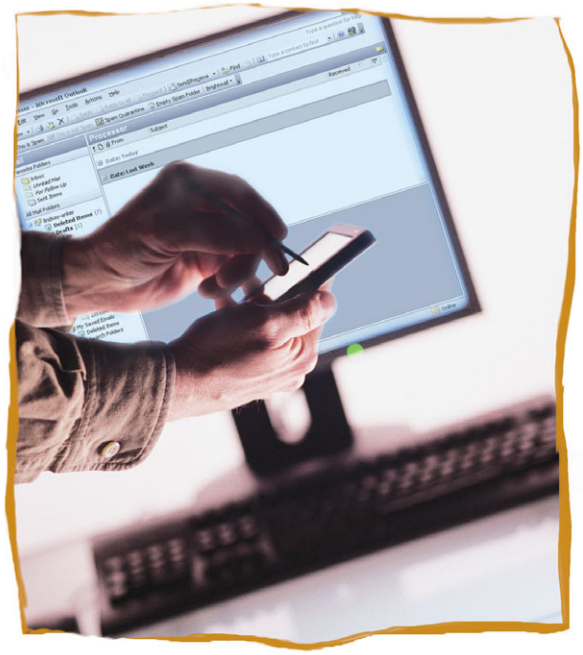
To help make the comparison between Wi-Fi, EVDO, and EDGE a bit easier, here's a summary of the main factors to consider with each type of wireless access.

	Wi-Fi	EVDO	EDGE
Speed	802.11b: 11Mbps 802.11g: 54Mbps	Sprint: 400 to 700Kbps with peak rates up to 2.0Mbps Verizon Wireless: 400 to700Kbps	Cingular HSDPA: 400 to 700Kbps on the downlink and bursts to more than a megabit per second Cingular EDGE: 70 to 135Kbps T-Mobile: Up to 168Kpbs
Availability	Wherever a hotspot is available	Sprint: 466 major U.S. airports coast-to-coast and 220 cities with a population of 100,000 or more Verizon: Available to more than 150 million Americans from coast to coast	Cingular BroadbandConnect: 52 communities Cingular EDGE: 13,000 cities and towns and in areas along 40,000 miles of highways T-Mobile: GPRS or EDGE available everywhere T-Mobile has coverage, Total Internet provides access to 7,000 HotSpots
Cost	Varies depending on the network you are accessing; some networks are free	Sprint: $59.99 per month* Verizon Wireless: $59.99 per month*	Cingular: Unlimited Data Connect plan for $79.99 per month* T-Mobile: $49.99 per month*
Equipment Required	Wireless network interface card, integrated in many notebooks, and also available as an internal PC card or external USB device	Compatible PC card or phone	Compatible PC card or phone
Security	Depends on the connection	Generally, more secure than Wi-Fi	Generally, more secure than Wi-Fi
Range	Depends on local obstacles and distance from access point	Available wherever you can receive a cellular signal	Available wherever you can receive a cellular signal
Strengths	Allows multiple computers to share an Internet connection Generally affordable Widespread availability, with daily expansion	More secure than Wi-Fi Seamless roaming between towers Widespread availability, with daily expansion	More secure than Wi-Fi Seamless roaming between towers Widespread availability, with daily expansion
Weaknesses	More susceptible to security breaches than other connections Fixed locations	Costly Unavailable in some areas	Costly Unavailable in some areas

**Qualifications may apply*

Access Email From Your PDA

Wherever You Go, Your Inbox Is There



While pecking out emails with your thumbs definitely gets old fast, the ability to check your email from a baseball game, commuter train, or grocery store doesn't. Accessing email from your PDA means that you can, essentially, carry your inbox in your pocket. And, like your mobile phone or ATM card, once you start getting email on your PDA, it's hard to imagine how you ever lived without it. To help you access your personal email from your PDA, we'll walk you through the setup process for four models from a variety of major carriers.

BlackBerry 7130c (Cingular)

In order to receive email on your BlackBerry 7130c ($199 with contract; www.blackberry.com), you must first create a login ID and password, which you can do either from your handheld, or from a computer.

To set up email directly from your BlackBerry, start by connecting to the Cingular network. If the words "EDGE" or "GSM" appear next to the blue bars in the top right corner of the home screen, you're connected. If those words and bars do not appear, click the Tower icon on your home screen to connect to the network.

Once connected, the Sign In screen may appear automatically. If it doesn't, click the Personal Email Set Up icon—it looks like two envelopes under two interlocking gears—select Create New Account, and then click Get Link. You'll be asked to read a user agreement. Once you've done so, click I Agree and, when prompted, enter a User ID. This will become your login name for the BlackBerry Internet Service Web site. Create a password, confirm it, and click Next.

At this point, you'll be asked to enter your full email address (for instance, JonBlack@ISP.com) and password in the appropriate fields. Once you've done this, click Next. If everything looks correct, click OK.

To set up your email using a PC, start by going to www.cingular.com/blackberrystart. (If a service upgrade has been made available, or if there is other news that Cingular deems important to users, you may need to make one extra click to skip the news and get to the login page.) Once at the login page, click Create New Account. You'll be asked to agree to the terms of use, and once you have, you'll also be asked for the PIN and IMEI (International Mobile Equip-ment Identity) number for your handheld device.

To find your PIN and IMEI, click the Settings icon (a folder full of gears) on your BlackBerry. Then click the Options icon (two interlocking gears), and scroll down the alphabetical list to select Status. Your PIN and IMEI should appear—clearly labeled—along with some other basic data about your handheld.

Once you've entered your PIN and IMEI number, click Continue, create a User ID and password, and from there, the steps are the same as above.

Once the setup process is complete, checking your email from your BlackBerry 7130c is a cinch. Push technology will automatically send your email directly to your handheld as it arrives. You can receive mail from up to ten accounts, each of which can be configured separately and assigned a "sent-from" address, auto-signature, and filter.

An envelope icon will appear on the home screen of your device for each of your email accounts. When you move your cursor over an email icon, the address will be displayed just underneath it, along with the number of new messages. Simply click it to visit your inbox. To read an email, click it, and from the pop-up menu, choose Open.

For personal email accounts, BlackBerry Internet Service directly supports POP (Post Office Protocol) and IMAP (Internet Message Access Protocol) accounts, Microsoft Outlook, and web-based mail clients such as Gmail. For certain kinds of work email, such as IBM Lotus Notes accounts that must be retrieved from behind a corporate firewall, additional

software (downloadable from BlackBerry Internet Service) is required.

Palm Treo 700p (Sprint)

There are several ways your Palm Treo 700p ($399.99 with contract; www.palm.com/us) can retrieve email. Because it has a built-in Web browser (like the other PDAs and smartphones we've included here), you can check your Web-based mail from your handset in essentially the same way you would from any other browser. There are also two Sprint applications specifically designed for business Treo users who want to access secure corporate accounts. Because we want a quick, easy way to check our personal email (from providers such as AOL, Comcast, or Earthlink), the best bet for us is VersaMail, which is preinstalled on your Treo.

To configure VersaMail, press the Applications button (it looks like a house) and then tap the Email icon. From there, tap Continue and give your account a descriptive name, such as "Home Mail." Below the Account Name field is a pull-down menu labeled Mail Service. Scroll through the names until you find your email provider, and then click Next.

In the Username field, enter the username for your email account. If you're not sure what your username is, try the first part of your email address (everything before "@"). In the Password field, select Unassigned, click OK, and then click Next. VersaMail will supply you with the incoming and outgoing mail servers for your account. Click Next and then click Done.

Before the setup process is completed, you may be asked if you want to overwrite the existing settings for this account. While it seems counterintuitive, your answer to this question is actually "Yes." Click Yes, then click OK, and you'll be taken directly to your newly created Inbox.

To start retrieving messages, click Get. If you are asked if you want to turn the phone on, or if you want to connect to the Internet, answer in the affirmative. Because email is not pushed to your device, you'll only get access to your new messages if you ask for them. To do this at any point, click the Applications button on your keypad, click the Email icon, and then click Get. If an incoming message is truncated, which happens automatically to mail over a certain size, click More.

The ever-popular BlackBerry keeps you close to your email, no matter where you are.

The Palm Treo 700p's keypad makes it easy to compose email as well as receive it.

HP iPAQ hw6900 (carrier TBD)

The HP iPAQ hw6900 ($929.99; www.hp.com) is so new that at press time, a prototype wasn't even available to the product managers at HP (it's expected to ship by the end of the year). Because it is a Windows Mobile 5.0-based PocketPC that enables push email capabilities, receiving email should be a breeze. Users will have several options, including synchronizing with Outlook, Pocket MSN for Hotmail, and Xpress Mail Email, which is available in versions customized for business or personal users.

To set up your personal email on your iPAQ hw6900, tap Start, and select Messaging. Next, choose Menu, Tools, and New Account. Enter your email address, and tap Next. The auto-configuration feature will attempt to download your email server settings. When it is finished, tap Next, enter the name you want displayed when you send email, then enter your password.

If the auto-configuration was successful, your username will already be entered and you can tap Next, then Finish, to complete setting up your account. Tap Options to adjust the settings for things such as attachments, the number of messages that are downloaded, or how often mail will be downloaded.

If your iPAQ was unable to configure your account automatically, you'll be asked to enter the account settings, such as username and password, manually. To do this, tap Start, Messaging, and select an account. Click Menu, then Options, then New Account. In the Your Name field, enter the name you would like displayed when you send email. In the Email Address field, enter your email address, then tap Next. You may be prompted to enter other information, such as mail server names. When the Finish option becomes available, click it to complete the setup process.

Once your account is set up, you'll be able to access your email from the Today screen. Outlook users can

simply click the Outlook email icon. For non-Outlook accounts, such as Gmail or AOL, click the envelope icon, and select your account from the list.

T-Mobile SDA (T-Mobile)

The T-Mobile SDA (Smart Digital Assistant) is the first smartphone from T-Mobile based on the Windows Mobile 5.0 platform. You can configure your T-Mobile SDA ($299.99; www.t-mobile.com) to receive mail from Hotmail, AOL, Yahoo! Mail, Comcast, and any other POP3 or IMAP4 mail server. To set up your account, from the Today (home) screen, choose My E-mail, and then select Add A New My E-Mail Account. Click Next, then enter your email address and password. (The period that you'll need to create the "dot" in your email address is not shown on the face of any of the keys on your handset. To insert a "dot," press the "1" key once.)

If you'd like your device to remember your password, check the Save Password box. If you don't do this, then you'll have to manually enter it every time you want to access your mail. To finish the email setup, choose your time zone from the pull-down menu, and click Next. If you have any trouble, the My E-mail setup wizard will let you know and walk you through some additional steps. You'll be able to check for and correct any typos in the details you entered. If setup still fails, you may need to manually enter the server type and name.

Once you're up and running, to check your messages, return to the Today screen, click the envelope icon, and select your account from the list. This will take you to your inbox where your new mail should be waiting.

A Word About Gmail

If you're a Gmail user, before you can receive email on your handheld device, you may need to make an adjustment to the way your Gmail account is configured. To do this, go to www.gmail.com to access your Gmail account, click Settings, then select Forwarding and POP. In the POP Download box, select one of the Enable POP options. (You can either enable POP for all the mail you've ever received, or for mail that arrives from the time you enable the POP until you disable it again.) Click Save Changes. For help configuring Gmail with mail clients, such as Outlook, which you can sync with Windows Mobile devices, click the Configuration Instructions link (item 3 in the POP Download list.) You'll also find instructions for configuring your BlackBerry to receive Gmail.

No matter which device you choose—a Windows Mobile, Palm, or BlackBerry—it will only take a matter of minutes to get your personal email up and running on your handheld. We can't say how long it will take to become proficient at typing with your thumbs, but we're certain that the learning curve is worth it. RS

BY NAOMI GRAYCHASE

Use A Windows Mobile 5.0 PDA To Access Files

In the thirteen years since Apple first coined the term "PDA," and BellSouth began selling the first smartphone (the Simon), PDAs have evolved into devices that do almost as much as our PCs. In addition to PIM (personal information manager) tasks, such as managing your calendar, address book, and task list, with today's PDAs you can browse the Web, send and receive email, open documents, play games, and even use applications such as translators or mapping software.

One of the perks of opting for a PDA running Windows Mobile 5.0 is that for Windows users, the interface is very familiar. From the Today screen, selecting the Start button lets you open programs; or use File Manager to access the My Documents, My Music, My Pictures, and Program Files folders, as well as any other folders or files you have created.

With versions of popular Microsoft applications designed specifically for PDAs—Outlook, Excel, Word, and PowerPoint, for instance—you can send and receive files, as well as create and edit documents, spreadsheets, and presentations from your handheld in very much the same way that you would on your desktop or laptop system.

The mobile versions of Office programs are currently available on Pocket PCs and phone-enabled Pocket PCs (such as the Palm Treo 700w and T-Mobile MDA), but not on Windows Mobile-powered smartphones (such as the T-Mobile SDA). Outlook Mobile is built into Windows Mobile 5.0 and fully supports Word, Excel, and PowerPoint attachments. It doesn't have the robust functionality of the full desktop version, but it can do the essential tasks, including allowing you to create emails while offline for delivery later. Using ActiveSync, you can easily sync your Windows Mobile PDA with your primary system to help keep the contacts, calendar, and other data in your handheld current.

To download large data files, many new devices, such as the HP iPAQ hw6900, offer built in Wi-Fi so that you can get broadband Internet access via the nearest hotspot.

Windows Mobile-based Pocket PCs support Adobe's digital edition technology files (eBooks), so you can download and read electronic versions of books, magazines, or newspapers on your PDA, as well. And as an open platform, Windows Mobile lets you download third-party games, applications, and utilities to your heart's content.

Phoning Home

Connect To Your PC From The Road

Networking has always been important in the business world. We're not talking about social networking here, but the ability to share information among all employees whether they work in the corporate headquarters or a small branch office. Over the years, technology has made it easier and cheaper to keep businesses connected. Many of those technological advances have made their way to the home sector as well, allowing the home user to stay connected to their home PC while on the road.

A History Lesson

The need to connect one computer to another has been around almost as long as computers. Before the advent of the personal computer, companies maintained large mainframes that connected to various terminals throughout the office. Employees used a terminal to work with the mainframe.

The PC ended the golden age of mainframes, but users still wanted access to remote PCs through a network. Before the rise of the Internet, many companies bought leased lines from the phone company to connect branch offices. While expensive, these leased lines allowed companies to create a secure, private WAN (wide-area network).

The Internet provided companies with an alternative to expensive leased lines. Using the Internet, companies could encrypt data to protect sensitive information while it travels over the public Internet. Remote access tools have come into the Internet age.

Although often developed with businesses in mind, many remote access tools are available for personal use as well. Creating a remote connection to your home PC, however, poses special challenges. As you know, every system on the Internet must have a unique IP (Internet Protocol) address (which consists of four sets of numbers between 0 and 255 separated by a period). Most businesses have a static IP address that never changes while most home users have a dynamic IP address that changes at specific intervals. In order to connect to your home PC, you need to know what IP address it's currently using. Home routers can add a bit more complexity by obscuring your desktop computer's IP address. As a result, finding your desktop computer on the Internet is next to impossible without some sort of added intervention.

Remote Access Options

There are two main types of remote access tools for the home user: VPN (virtual private network) and remote control software. VPN is often complicated to set up and, as a result, more of a business tool. Nonetheless, some companies allow employees to access the company network from home via a VPN connection. Remote control software is a better option for someone looking to access their home desktop while on the road.

VPN. VPN is very secure, but as we mentioned above, it can be difficult to set up. You can establish VPN connections between your remote PC and the company network or between two networks (for instance, between a branch office and the company headquarters). A VPN requires a VPN server (which provides access to the remote computer) and a client (which you use to access the remote computer). To connect to a VPN, you need an IP address for the VPN server. This makes using VPN at home difficult as the IP addresses on home PCs often changes.

Most VPNs use a process called tunneling to create a private connection. Tunneling essentially hides the

original data in several different layers. The original data, or Passenger Protocol, is hidden within an Encapsulating Protocol. A Carrier Protocol then encloses the Encapsulating Protocol and carries the data over the Internet.

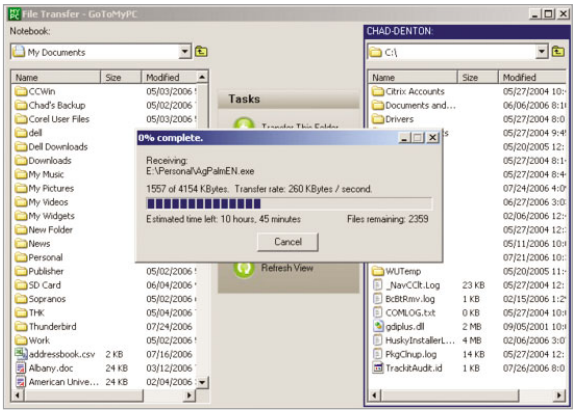
To illustrate the process, imagine the Passenger Protocol is a letter with sensitive customer information. Before sending the letter, you place it in a standard envelope (the Encapsulating Pro-tocol). You then place the envelope in a larger manila envelope (Carrier Protocol). You address the manila envelope to its recipient and send it on its way. When the packet arrives at its destination, the recipient removes the smaller envelope before opening the letter.

If your company allows VPN connections, check your system administrator for instructions on how to configure a VPN client on your computer. Windows XP includes its own VPN client, but it may not be compatible with all VPNs. To learn more about VPN, see "Tunnel Into Your Network With VPN" on page 102.

Remote Control Applications. Compared to VPNs, remote control applications are relatively simple in design and easy to set up. It's also much cheaper than setting up a VPN and often a better choice when working with slower connections.

As we mentioned, your home connection's dynamic IP address makes finding your computer on the Internet difficult. To overcome this problem, most remote control software uses special servers to track IP addresses. For instance, if you want to access your desktop at home from your notebook, you'd install client software on both the notebook and the desktop. When the desktop is on, it will connect to the server and provide its current IP address. When you turn on your notebook and log into the service, your notebook provides the server with its IP address. The server can then inform both systems that the other is online and available.

Remote control software provides you with complete control over the remote computer. You can open and use applications installed on the remote computer, troubleshoot software on the remote system, and, in most cases, transfer files between the two systems.



File transfer is a major benefit in a remote access tool. GoToMyPC lets you transfer files between the host and client computers. It sports a simple, intuitive interface.

Remote control software also works great with limited bandwidth (such as dial-up connections). Sending screen shots along with mouse and keyboard movements is relatively easy even on a dial-up connection. You may notice some irritating lag when using dial-up, but it will still work properly.

Remote control software does have some security drawbacks. In most cases, password authorization controls access to remote systems. Using a weak password to protect your system is like leaving the front door to your house unlocked. Once unwanted visitors gain access to your system, they'll have complete control over the system and all the files and folders on it.

There is another security concern depending on how the remote control software works. Some applications require you to send information to a server. The server will then forward the data to the remote system. You have no control over the server and it's always possible that someone is looking at your information as it passes through the server.

Get Connected

Remote control software is available at a variety of prices. In fact, Windows XP Professional includes a Remote Desktop feature that allows users to access the system over the Internet. In order to use Remote Desktop, you'll need to configure Remote Desktop on your WinXP Pro system and make sure the Windows Firewall is set to allow Remote Desktop connections. You'll also need Windows 95 or newer and Remote Desktop Connection software on the PC you'll use to connect to the remote system. You can also use Pocket PCs and smartphones to connect to your remote system.

In order to use Remote Desktop, however, you'll need a VPN connection between the remote system (the host) and the system you're currently using (the client). If you don't have a VPN connection, you might still be able to connect, but you'll need an IP address for the host. This makes the Remote Desktop option difficult to use if the host has a dynamic IP address.

If you're not running WinXP Pro, don't have a VPN connection, or you just don't want to run Remote Desktop, Hamachi is one alternative. Hamachi (www.hamachi.cc) makes it very easy to connect to a remote desktop even if the host has a dynamic IP address (and even if the system is behind a home-networking router). To use Hamachi, you need to install the software on both the host and the client. The software on the desktop logs into the Hamachi servers and receives a Hamachi-specific IP

address that you can connect to from another computer with the Hamachi client installed. There is a security concern when using Hamachi because the software is not open source (so others can't evaluate the software's trustworthiness) and all information needs to pass through Hamachi's servers. Hamachi is also currently in beta, so there may be security related bugs in the software.

Hamachi, however, is very easy to set up and lets you run any application that you can run through a LAN (local-area network). For instance, using Hamachi, you can access your music through iTunes while on the road. You can also transfer files between computers over the Internet using Hamachi. The software is free to download and use.

Other commercial applications are also available. One of the most popular, GoToMyPC (www.gotomypc.com), is also one of the most expensive. The Personal Version from Citrix Online (www.citrixonline.com) costs $19.95 a month for one computer. A free 30-day trial of the service is available.

GoToMyPC is a very intuitive and full-featured program. To begin, you need to install a small application on the host computer. After installing the software, you'll need to take a few seconds to register the host with the service. Once configured, you can access the host by opening a Web browser on any other computer and logging into your account at the GoToMyPC Web site. After installing a small Java-based viewer, the host's desktop appears in the browser.

The $19.95 plan allows you to have one PC configured as a host at any one time. You can always delete a configured host and install the software on another PC if you need to.

In addition to accessing, editing, and transferring files, you can perform other functions; for instance, you can reboot the remote system (although this will disconnect you from the remote system). GoToMyPC is perfect for troubleshooting and working with network applications on the remote system.

Once you've become accustomed to remote access, it's difficult to do without it. Keep these services in mind the next time you need to check your work email from home or want to upload images from your vacation to your PC at home. RS

BY CHAD DENTON

Configure GoToMyPC

Although expensive, GoToMyPC is one of the easiest remote access tools to use, and you can get a free 30-day trial if you want to kick the tires a bit before paying good money for it.

Start by visiting https://www.gotomypc.com. Click the Try It Free button (or the Buy Now button if you want to skip the free trial) and enter your name and email address. You'll also need to enter a credit card number and billing address even if you're signing up for a free trial. If you don't cancel the service, GoToMyPC will automatically bill you $19.95 when the 30-day trial is over.

After you sign up for the account, you'll have the opportunity to download and install the GoToMyPC software. Make sure you install this software on the computer you want to be able to access remotely (the host). After installing the software and rebooting the PC, you'll need to register the host with GoToMyPC. Provide the email address and password you created when signing up for GoToMyPC and click OK. Next, provide a Nickname for the PC and an Access Code. The Access Code should be at least eight characters long and consist of letters and numbers. Remember this code as you'll need it to complete the connection later. Click OK to finish registering the computer. A Web browser should open with further instructions. You can close the browser if you prefer.

To log into the remote system, open a Web browser on another computer and visit https://www.gotomypc.com. Enter the email address and password you provided when creating the account. You should see the currently registered computer in your Computer List. Click the Connect button to initiate the connection. When prompted, provide the Access Code you chose when registering the host PC.

You should see the remote system's Desktop appear in your GoToMyPC window. Depending on the resolution of the remote system, GoToMyPC may reduce the size of the remote display. This may make the display look a bit fuzzy. If that's a problem, click Actual Size in the view menu (you can scroll through the display using the mouse).

You can click items displayed in the remote Desktop just as if you were in front of the remote computer. For instance, clicking the iTunes icon opens iTunes on the remote Desktop and provides you with access to your music. You can also open Word, Excel, or nearly any other application. You can modify existing files or create and save new files. To transfer a file between the two systems, click the File Transfer button (the folder icon) in the upper-right corner. To close the connection, click the green X in the upper-right corner. When asked if you really want to quit, click Yes.

To designate another computer as the host, log in to https://www.gotomypc.com, click the name of the older host, and click the Delete button. You'll now be able to install the host software on the new system. You will need to repeat the registration process on the new host. ❙

Tunnel Into Your Network With VPN

Take Your Office With You

Before the Internet and broadband technology came along, companies had to pay lots of money for private communications between remote computers and their corporate networks. Today, VPNs (virtual private networks) use the power of the Internet and security technologies to protect sensitive information. Thanks to VPN technology, if you telecommute or travel, you can access your company's network from home or while on the road (whether you want to or not!). And as VPN technology spreads to more types of network devices, you can even access some small or home-based networks remotely.

Traditionally, larger companies have been the main users of VPN technologies. With a VPN connection, remote workers can securely log on to a corporate network. VPNs also allow secure network-to-network connectivity, such as a branch office network securely communicating with a main office network.

With the increasing use of high-speed Internet connectivity and new low-cost, entry-level VPN devices, VPNs have become more practical for SOHO (small office/home office) users. In this article, we take a closer look at VPNs and how SOHOs can use them.

Is A VPN Right For You?

A VPN makes sense for SOHOs with mobile employees who regularly need access to the company network from remote locations. Also, if you are frequently away from your home office and need secure access to your home network, a VPN can help you get into your network anytime, day or night.

A VPN can include both monetary and productivity costs. If you have a typical small network with a router or wireless AP (access point) connecting several PCs, you will likely need to purchase additional VPN equipment. Depending on how it's configured and the equipment you choose, a VPN can slow down your network's performance. And working on your network over a VPN connection is definitely slower than working directly on the network.

How It Works

A VPN creates a private, secure "tunnel" from one endpoint to another endpoint. The endpoints can be a remote user's notebook computer to a **network gateway** (client to gateway). A network gateway is a designated entry point into a network, such as a router or wireless AP. Another endpoint configuration for a VPN is connecting a network gateway in one location to a network gateway in another location (gateway to gateway). This article focuses on a client-to-gateway scenario for mobile, remote access to your SOHO network.

To create the secure tunnel, a VPN uses a variety of technologies that support encryption, authentication, and/or data integrity. **Encryption** is the process of making information unreadable to unauthorized users by converting it to cipher text. **Authentication** ensures that users attempting to access your network are who they say they are. Authentication methods include passwords, usernames, and PKI (public-key infrastructure; a means of verifying users and network devices). **Data integrity** guarantees that the transmitted information is not altered or tampered with.

The common **protocols** (rules of communications between computer systems) for VPN connections are PPTP (Point-to-Point Tunneling Protocol), L2F (Layer 2 Forwarding) protocol, and L2TP (Layer 2 Tunneling Protocol). Of these, L2TP is generally the recommended protocol for remote access directly to a VPN gateway on a network. Less common are the SSL (Secure Sockets Layer) and TLS (Transport Layer Security) security protocols that are also known as Web VPNs. This type of VPN is a newer type of implementation that has not yet trickled down to the SOHO market.

L2TP is usually protected by IPsec (Internet Protocol security). **IPsec** is a collection of security protocols defined by the IETF (Internet Engineering Task Force; www.ietf.org). IPsec provides encryption, authentication, and data integrity to secure data transmissions. Because it provides the highest

level of security, the L2TP/IPsec combination is the best choice if you are implementing a VPN for remote user access to a network.

What You Need

To implement a VPN, you need two endpoints with VPN capabilities. One end is the VPN gateway. The other end can be another VPN gateway to bridge two networks, or it can be a client in the form of a notebook or laptop PC for remote access to the network when you're telecommunting or traveling (the focus of this article).

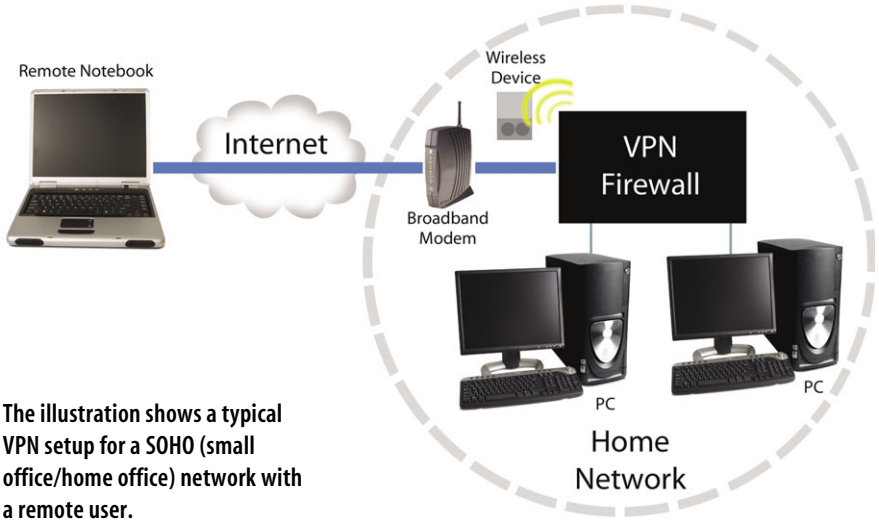
For practical purposes, you also need an always-on broadband Internet connection for your network. A dial-up connection is too slow and is not continuously available.

Gateway. For a SOHO scenario, the easiest method of providing VPN access to your network is a gateway device, such as a router or firewall. Because firewalls already have numerous built-in security features, they are the most common method of implementation.

Although VPN endpoint support is included in some SOHO network equipment, it is not a common feature. If your network already has a firewall device or router, the device probably does not include VPN endpoint capabilities. Note that if you check the device's specs, you may see VPN pass-through listed as a feature. **VPN pass-through** means that the device allows VPN traffic to pass through it. This is different from the ability to offer VPN endpoints or tunnels to remote users.

Examples of VPN gateway devices for the SOHO market include:

- NETGEAR FVG318 ProSafe 802.11g Wireless VPN Firewall 8 ($179.99; www.netgear.com)
- NETGEAR FVS318 Cable/DSL (digital subscriber line) ProSafe VPN Firewall ($129.99)
- D-Link Express EtherNetwork VPN Router DI-804HV ($59.99; www.dlink.com)



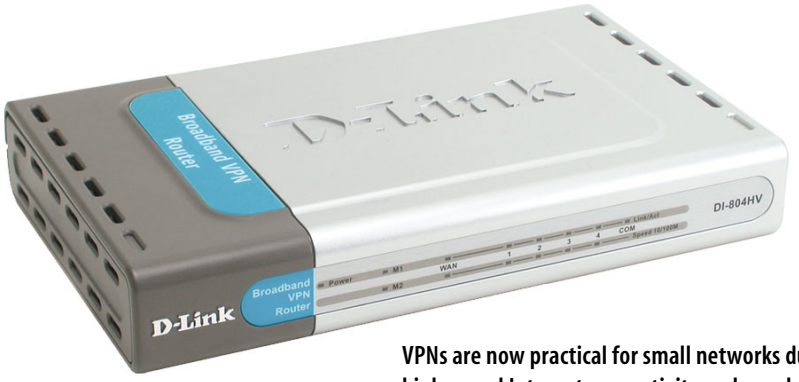
The illustration shows a typical VPN setup for a SOHO (small office/home office) network with a remote user.

- D-Link DI-824VUP AirPlus XtremeG Wireless 802.11g VPN router ($159.99)
- SonicWALL TZ 150 Wireless ($429; www.sonicwall.com)

All of these devices include a router, firewall, and Ethernet connections for PCs and other network devices. The wireless devices also include an 802.11g wireless AP. For VPN connections, they feature support for IPsec, L2TP, and multiple simultaneous tunnels so that more than one remote user can establish a VPN connection at the same time.

The NETGEAR and D-Link devices are most appropriate for smaller operations where the remote users are logging on using a notebook or PC that you know is secure, virus-free, and known to the network. The SonicWALL TZ 150 device offers more advanced security features, including antivirus, antispyware, intrusion detection, and wireless guest services. It also comes with hardware acceleration to offload the processor-intensive encryption routines. Some of the TZ 150's security features are purchased separately in the companion gateway software bundle ($145).

Client software. In order for a remote notebook or desktop computer to connect to the VPN gateway, it needs to be able to understand the VPN protocols. Vendor software is available to



VPNs are now practical for small networks due to high-speed Internet connectivity and new low-cost, entry-level VPN devices, such as this D-Link Express Ethernet VPN Router DI-804HV.

handle this, and the Windows OS (operating system) includes support for some of the VPN protocols. There are also third-party products available.

Vendors such as NETGEAR, D-Link, and SonicWALL normally create companion client software for their VPN network devices. The software is designed to easily integrate with the vendor's VPN devices. It may also include other features not available in the Windows OS. However, vendor client software is not free; you'll pay $40 to $50 per copy, and you need to install it on each computer that will access the VPN.

Windows 98/Me/2000/XP PCs come with support for the PPTP protocol. As we noted earlier, however, most VPN experts recommend using the L2TP/IPsec protocol. Only WinXP/2000 offers built-in support for L2TP/IPsec.

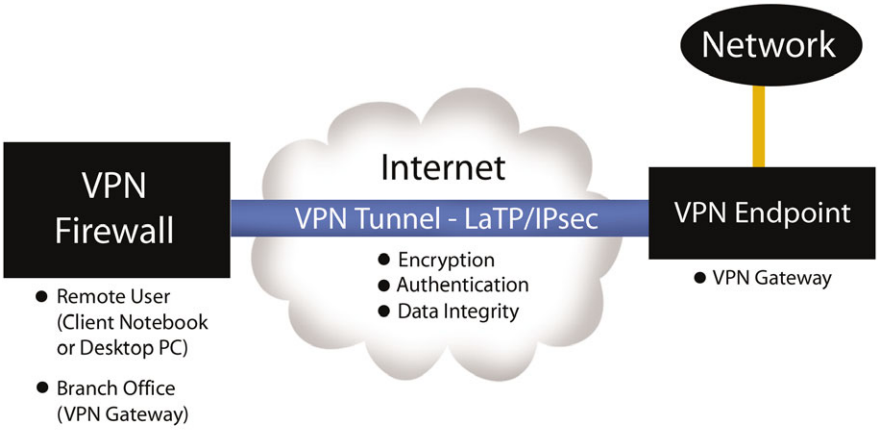
An example of a third-party VPN client program is SafeNet SoftRemote ($149; www.safenet-inc.com). SoftRemote is compatible with most Windows OSes, and it offers additional features such as policy management and support for smart cards.

If you don't need a lot of extra features and your remote computers run WinXP, you can try the built-in VPN support in WinXP. If you need additional features and want an integrated solution, the software provided by the manufacturer of your hardware VPN is the way to go. And if the hardware manufacturer's software doesn't provide everything you want, third-party programs are another option.

How to Set Up An L2TP/IPsec Remote User VPN

Configuring a remote user VPN is a three-part process. The first part of the process is configuring the VPN gateway device. Then you need to configure your remote computers to access the VPN gateway. The final step is testing the VPN connection.

Connect and configure the VPN gateway. Specific instructions for configuring your gateway device are best acquired from the documentation available from the vendor. However, a number of configuration tasks and VPN-related settings apply to most devices.



A VPN consists of two endpoints, with a secure, protected tunnel between them. One endpoint can be a remote user or a branch office network that establishes a VPN connection with a main network as the other endpoint.

To begin, you must connect the device to your existing network. If your current network router or wireless AP does not support VPN, you can replace it with a new VPN firewall/router similar to those we noted previously. We also assume you have a high-speed cable or DSL modem for Internet access.

Turn off all equipment and connect the modem to the VPN firewall/router, and connect the router to the Ethernet port of the main computer (the computer that was connected to the Internet when the modem was originally installed). Plug in and turn on the modem and wait a few minutes. Next, plug in and turn on the router, and then turn on your computer. Verify the appropriate indicator lights—for example, Power, Internet, LAN (local-area network), and Wireless—are activated on the router.

To configure the firewall/router, most vendors supply a Web-based administration tool that you access from a computer connected to the device. When you open the Web browser on that computer, the configuration screen may automatically display. If not, refer to the documentation from the device vendor and enter the appropriate Web address in your browser to access the router's configuration screen. Follow the vendor's instructions for logging into the device's administration tool. Configuring the device entails more than VPN settings; however, we'll focus on VPN-related tasks here.

Defining the VPN information involves creating a security profile for both endpoints of the VPN connection. You will create a security profile for the VPN firewall (gateway) device and the VPN client, so that each endpoint can identify the other. The VPNC (Virtual Private Network Consortium) recommends specific settings for certain parameters, as seen in the chart, "VPN Settings."

The VPNC (Virtual Private Network Consortium)-recommended settings provide the best security for most systems. However, there are productivity tradeoffs. For example, 3DES (triple DES; a cipher or code for encrypting information) is slower but more secure than DES (Data Encryption Standard), and SHA-1 (Secure Hash Algorithm-1; a formula for

VPN Settings

Parameter	Setting
Secure Association	Main Mode
Authentication Method	Preshared Key
Encryption Method	3DES
Authentication Protocol	SHA-1
Diffie-Hellman (DH) Group	Group 2 (1,024 bit)
Key Life	8 hours (28,800 seconds)
IKE Life Time	24 hours (86,400 seconds)
NETBIOS	Enabled

Source: NETGEAR

authenticating information) is slower but more secure than MD 5 (Message Digest 5; another type of algorithm or formula for authenticating information). Also note that the settings above are not all-inclusive, and your VPN configuration settings will contain additional parameters.

Depending on how your VPN firewall/router manufacturer handles configuration settings, you may also need to consider whether your home network connects to the Internet with a **dynamic IP (Internet Protocol) address**. ISPs (Internet service providers) generally do not assign a single, static IP address to your network for Internet access. Instead, the IP address changes periodically (a dynamic IP). This can become an issue when a remote user wants to connect to the network through the VPN, because the remote user's system doesn't have a fixed IP address to go by.

Vendors recommend different methods to handle dynamic IP addressing. You can use a dynamic DNS (Domain Name System) service to assign a domain name to your VPN firewall. Service providers include www.tzo.com and www.dynDNS.org, and the assigned name will be something like *mycompany.tzo.com* or *myname.tzo.com*. Different devices handle dynamic IP addressing in different ways, so it's best to refer to the product documentation for recommendations.

A remote computer's VPN client software will need the gateway's security profile so that the remote computer can connect to the VPN gateway. Before you configure your remote computer, note the following information from the VPN gateway configuration:

- Preshared key
- VPN tunnel/connection name
- VPN device IP address
- LAN subnet mask

You'll also need the information you entered for the parameters noted in the VPN Settings chart.

Configure the remote computer. If you're using a vendor-supplied or third-party VPN client software program, follow the product documentation to enter the security profile information for the VPN gateway.

If you want to try using WinXP to connect to the VPN, click Start, Control Panel, and Network And Internet Connections. Click Create A Connection To The Network At Your Workplace in the Pick A Task section to display the Network Connection Wizard. Select Virtual Private Network Connection and click Next. Type a Company Name (this does not need to match the VPN connection name), and click Next. Select Do Not Dial The Initial Connection and click Next. Type the IP address of the VPN gateway and click Next. Note that if the gateway is a router or wireless AP, the IP address is the same as the IP address you type to open the device's Web-based configuration tool. Select Add A Shortcut To This Connection In My Desktop if you want a shortcut for the VPN connection and click Finish.

In the Control Panel, click Network And Internet Connections in Category view, and then click Network Connections to display the computer's list of network connections. Right-click the VPN connection you just created and click Properties. Click the Security tab and select the IPsec Settings button. Select the Use Pre-Shared Key For Authentication check box and type the preshared key you defined for the VPN gateway. Save the new Property settings and close the dialog box.

Test it. Now that your VPN is configured, try to access your network through the VPN connection on the "remote" computer. Make sure the remote computer is connected to the Internet first, and then try connecting to the VPN. To initiate the connection, simply double-click its shortcut or System Tray icon.

If you are unable to establish a connection, double-check the VPN gateway and client configuration. Common issues include mistyped profile information or non-matching information. Also look for disconnected wires or no Internet connection. If you're using WinXP as the VPN client, it may or may not work well with the gateway device. You may want to try the router or wireless AP manufacturer's VPN client software instead.

Another possible problem is a personal firewall on the remote computer, such as Windows Firewall. Try disabling the firewall and connecting. If that works, then you need to create an exception for the VPN client software in the firewall settings. Check the VPN client software documentation for specific instructions.

Secure, Private Access

If your SOHO business can make use of a VPN, there's no need to wait. Today, you can purchase a VPN firewall with router features, wireless AP features, and more, for $60 to $500. Even if you don't think you need a VPN and you're in the market for a firewall, router, or wireless AP, consider purchasing one with VPN endpoint capabilities—you never know what the future might bring. RS

BY CARMEN CARMACK

Security & Privacy Essentials

Protect Yourself Online

Even though your computer may not contain thousands of credit card numbers, the names of CIA stringers, top-secret FBI information, or other highly sensitive data, it does contain *your* information. As a result, you probably don't want a stranger snooping on your computer, tracking your moves when you pay bills online, or sending emails from your account. For these reasons and many others, it's important to protect your computer from the outside world.

Even though most of us agree that network security is important, not all of us know how to secure our networks properly. Furthermore, even if you avoid online banking and similar (theoretically risky) activities, that doesn't mean that you and your computer might not be the victim of an attack. According to the Carnegie Mellon Software Engineering Institute, "Even if you have a computer connected to the Internet only to play the latest games or to send email to friends and family, your computer may be a target." If hacked, your computer could be used to attack other computers and bog down a network. Intruders could also send emails from your account or track your online activity and see everything you enter into a Web site—including passwords and credit card numbers.

Buckle Up

Just as you take a risk every time you get in a car and drive somewhere, you're taking a risk whenever your computer connects to the Internet. This risk is present regardless of your type of connection: dial-up, broadband, or via another network. But just as many of us refuse to stop driving simply because there's a chance we'll be involved in an automobile accident, giving up the Internet isn't something we're willing to consider either. In much the same way you protect yourself by putting on a seatbelt and driving safely, you can protect yourself on the Internet.

Instead of a seatbelt for your computer, you'll need a few basic tools to protect your PC against intruders. All operating systems and network connections should have a firewall, antivirus protection, antispyware protection, and—on wireless networks—encryption.

Firewall. A firewall makes your network invisible to the outside world. Think of it like an unlisted phone number. If your number is not available in the phone book, you're less likely to receive telemarketing and other calls from people you don't know. In much the same way, if an intruder can't see your computer or network, he is less likely to target you for an attack.

There are basically two types of firewalls: hardware and software. Hardware firewalls are built into many routers and are generally more secure than their software counterparts. If you only have one computer to connect to the Internet, cost may deter you from purchasing additional equipment that contains a hardware firewall. In this case, a software firewall, such as the one included with Windows XP, will help to protect you.

Generally speaking, software firewalls may not be as secure as hardware firewalls because they are more susceptible to "exploits" based on errors in other programs or in the OS (operating system) itself.

Every firewall will require some setup before initial use. Check with the vendor of your firewall if you require instructions specific to your firewall, or

read "Protect Your Network" on page 109. For the best security, install a hardware *and* a software firewall.

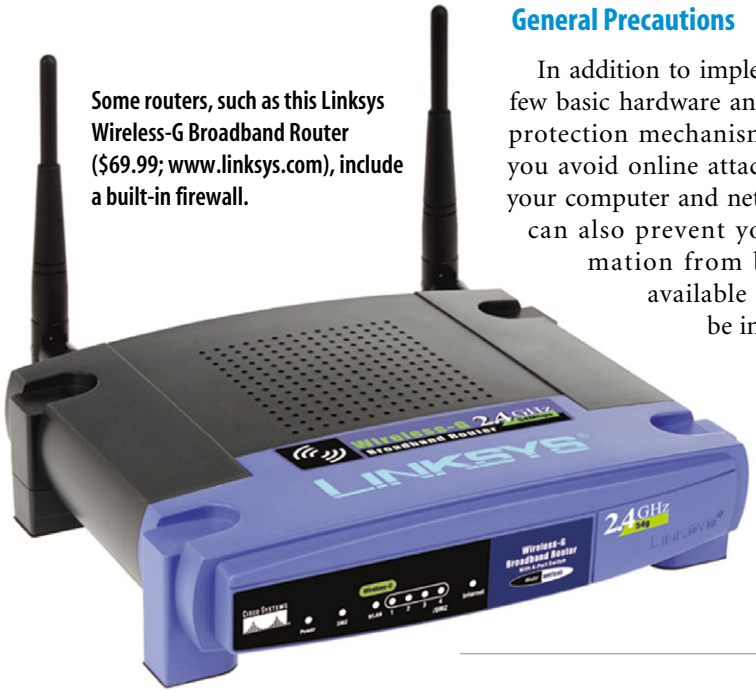
Antivirus and antispyware protection. Although antivirus and antispyware programs protect against different threats, the steps required to install and maintain them are similar. Antivirus software protects your computer from viruses that seek to destroy data or halt the operation of your computer. Antispyware software guards against spyware that could track your user behavior and send information about that behavior to outside sources without your knowledge.

Many antivirus and antispyware programs detect and block viruses and spyware by comparing known threat profiles to activity on your computer. These programs use definition files to identify known threats. Therefore, in order for your antivirus and antispyware applications to be effective, you must update the definition files on a regular basis. Many antivirus programs, including Norton Internet Security from Symantec, offer an automatic update feature for broadband users.

Most antivirus and some antispyware programs require a subscription for updates, and many of these subscriptions expire one year after you install the program. After the subscription expires, renew it or purchase and install new security software to ensure that your computer stays protected against new and emerging threats.

Wireless encryption. Due to their nature, wireless networks are more likely than wired networks to be compromised. Thus, wireless networks need an extra layer of security and privacy. You can achieve this added protection by using encryption. Two types of encryption are prevalent today: WEP (Wireless Encryption Protocol) and WPA (Wireless Protected Access). WEP is an older standard and tends to be more widely supported, especially by older equipment. Newer equipment generally offers both WEP and WPA encryption. Note that WPA provides stronger encryption than WEP.

Encryption is crucial to keeping your information safe. As Kendall Johnson, network administrator for Southeast Community College in Lincoln, Neb., notes, "Anyone within range of your unencrypted wireless network can use packet-sniffing software to intercept and view all information you transfer over your network, including your emails, Web sites visited, passwords, and credit card numbers."



Some routers, such as this Linksys Wireless-G Broadband Router ($69.99; www.linksys.com), include a built-in firewall.

General Precautions

In addition to implementing a few basic hardware and software protection mechanisms to help you avoid online attacks against your computer and network, you can also prevent your information from becoming available to would-be intruders by following a few general, sensible computing guidelines.

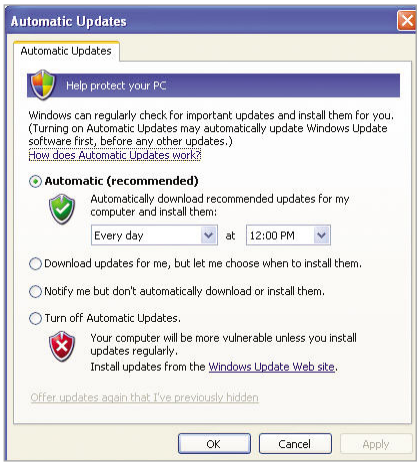
Use strong passwords. One of easiest ways to create a barrier between you and the outside world is to protect your computer by requiring all users to enter passwords before they can access information on the computer. For the best security, use a strong password and change it on a regular basis.

A **strong password** contains both upper- and lowercase letters and at least one special character, such as a number. Although it can make remembering your password more difficult, avoid using full words in your password. To create a secure password, think of ways you can combine dates, phone numbers, birthdates, places, or events into a phrase that you will remember but that would be hard for others to guess.

Limit yourself. Another way to protect your computer from outside attack is simply to prevent access to critical files. Limited user accounts can protect your computer by blocking you or someone else from installing malicious programs; they can also prevent would-be attackers from installing programs using your user account.

Limited user accounts do not have full rights to install programs, modify certain files, or even access some files and the Registry. As a result, users and intruders using these accounts are less likely to cause harm to your computer and network than are users with administrative rights.

In addition to protecting your OS, you can also protect your documents by creating an encrypted folder on your hard drive in which you can store important files that you don't want other users to access. Only the creator of an encrypted folder can access its contents; even the administrator of a computer cannot access these files. To encrypt a folder, navigate to it using Windows Explorer. Next, right-click the folder and select Properties. On the General tab, click the Advanced button. An Advanced Attributes dialog box will


Automatic Updates
Automatic Updates
Help protect your PC
Windows can regularly check for important updates and install them for you. (Turning on Automatic Updates may automatically update Windows Update software first, before any other updates.)
How does Automatic Updates work?
Automatic (recommended)
Automatically download recommended updates for my computer and install them:
Every day
at
12:00 PM
Download updates for me, but let me choose when to install them.
Notify me but don't automatically download or install them.
Turn off Automatic Updates.
Your computer will be more vulnerable unless you install updates regularly.
Install updates from the Windows Update Web site.
Offer updates again that I've previously hidden
OK
Cancel
Apply

Windows' Automatic Windows Updates function helps ensure that your computer has the latest patches to fix security vulnerabilities.

appear. Check the box next to Encrypt Contents To Secure Data to encrypt the folder and its contents.

Keep current. Many Internet attacks that compromise the security of your network occur because an attacker knows how to exploit the vulnerabilities in an OS or in a program installed on your machine. Software manufacturers typically issue updates to repair these vulnerabilities once discovered.

To reduce the possibility of holes in your computer's software security, be sure you update your computer regularly. Microsoft Windows Update (update.microsoft.com) is a good source for updates. Also, check for updates from other manufacturers of software you have installed on your machine.

Broadband users who are likely to forget to check for updates on a regular basis should consider setting up Automatic Updates in WinXP. With Automatic Updates, your computer will keep itself current with the latest patches. To enable Automatic Updates, click Start, Control Panel, Security Center, and Automatic Updates. When the Automatic Updates dialog box opens, select the radio button for Automatic and then choose the time frame and other options that will work for you. Finally, click Apply and OK to save the changes.

Back up. No matter how safe you are on the Internet and how much you try to protect your network, it's always a good idea to have a backup of your important data. Obviously, you hope you'll never need to use it, but you'll be sorry if you didn't create a backup and then turn out to need one. When creating a backup, be sure to include your email, address book, documents, pictures, and any other important files. Keep in mind that backing up your data (documents, photos, spreadsheet files, etc.) is actually more important than backing up applications, since you can usually reinstall the applications from the original CDs.

Block pop-ups. Pop-up windows and ads are not only annoying, they also pose a threat to your network. When a pop-up window appears while you're surfing the Web, it's easy to accidentally click one of the links. In doing so, however, you may open your computer up to an attack. Some pop-ups point to Web pages that can infect your computer with spyware and other malicious code. Unfortunately, all it takes in some cases is for you to visit the site. This malicious code can enter your system without your knowledge, even if you quickly close the Web page.

There are many free pop-up blockers to choose from. The Google and Yahoo! toolbars both include pop-up blockers. Some Internet browsers also include built-in pop-up blockers. Most of these pop-up blockers will let you disable the block for individual sites, in case you need to visit a legitimate site that requires a pop-up.

Use Your Judgment

In addition to setting up a variety of security measures on your network, you can also protect your information using a bit of common sense.

Keep quiet. Never give out private information such as your credit card number or Social Security number over email or via IM (instant message). Email and IM messages are not secure on any type of connection, so don't trust them to keep your information safe.

Under lock and key. When you visit a Web site and enter private information, make sure that you are communicating with that business using a secured connection. You'll know if the Web site you are visiting is secure by looking for "https" in the Address Bar and by noting the little yellow padlock in the lower-right corner of your Web browser. If the padlock is unlocked or missing, don't transmit your information.

Even if you've used the site before, it's always a good idea to make sure your current connection is secure. Server or browser problems can result in an unsecured connection, even if you had a secure connection in previous transactions. Check for security each time you enter information you're not willing to share.

Be stingy. Just because you like your neighbors doesn't mean that you need to share everything with them. This is especially true when it comes to a wireless network connection. Keep in mind that anyone on your wireless connection has access to your network. If you aren't willing to share all of the information on your computer with your neighbors, don't share your wireless Internet connections with them.

Lock It Down

Whether we like it or not, we live in a dishonest world, beset by crime and fraud. The Web is part of that world. As a result, you must protect yourself from attacks. Networks without security precautions in place are asking for trouble. High-speed Internet connections make it easier than ever for a cracker to exploit your computer and use information from it for malicious purposes. To protect yourself, put security measures in place on your network. RS

BY JENNIFER JOHNSON

Protect Your Network

Keep The Wolves At Bay With A Properly Configured Firewall

Like any other society, the Internet is a mélange of good and bad elements. For each saint on the Web, there's someone trying to break into your computer and mimic your identity, hijack your computer in order to deliver spam, or use it to attack other networks, leaving you to hold the bag. For most computers, the best solution is a properly configured firewall.

I'll Huff & I'll Puff . . .

Firewalls used to be the province of techies, but fortunately for us, it no longer takes a computer scientist to set up a firewall. Today's firewalls have well-designed management utilities and default settings that do a serviceable job of providing adequate security right out of the box. But installing a firewall without some planning won't keep your network secure; as the Three Little Pigs found out, the Big Bad Wolf can make easy work of a poorly built house.

Internet Traffic & Addresses

The *lingua franca* of the Internet is TCP/IP (Transmission Control Protocol/Internet Protocol). When you search for something on Google, your computer is sending packets of data to Google's server, packets that are packaged in the TCP/IP. The structure of TCP/IP is complex, but for our needs there are only two key facets we need to understand. TCP/IP consists of data and headers. The data is what we want Google's servers to receive, and the headers contain addressing information, both where the data should be delivered and where it came from.

For the purposes of implementing a firewall, we can largely ignore what data is carried in TCP/IP packets. Firewalls that can peer into a packet's data are more complex than necessary for most home networks. However, we do care about the *type* of data sent.

The header on a TCP/IP packet contains both the destination and source addresses of the packet in a 32-bit format similar to this: 192.168.1.1.

If you've set up a home network before or simply connected to the Internet, you may be familiar with this type of address. Each computer on a network needs a unique IP (Internet Protocol) address in this format. Think of this address as the address for an apartment building. Google's servers each have their own IP address, and your computer also has its own address. When you search with Google, you're sending a stream of packets to the address of one of the company's servers, and in reply it's sending a stream back to your address.

Ports Direct Data To The Appropriate Application

An IP address alone isn't enough information to properly send and receive data across the Internet. For example, you might be browsing the Internet while downloading a file from an FTP (File Transfer Protocol) server, or retrieving email from a mail server operated by your ISP (Internet service provider). If all of this data were simply addressed to your computer's IP address, your computer would have no way of knowing whether the data should be sent to your email client, your FTP utility, or your Web browser.

The solution is to use ports. Ports are numeric specifications that are part of the TCP/IP packet's header. There are over 65,000 ports available, and each port number is typically associated with a specific Internet service or application. For example, Web servers typically "listen" to traffic on port 80. When your browser sends a request for a Web page, the Web server's operating system looks for packets with port 80 specified in the header, and then forwards them on to the Web server's http application.

Firewall Filtering

What does all this have to do with setting up a firewall? In its simplest form, a firewall is merely a computer that filters out TCP/IP packets based upon their IP addresses and their port numbers. If someone sends a packet to

your computer, a good firewall will inspect the packet, check its ruleset to see if the packet should be allowed through, and then forward it to your computer.

Invisibility

A personal firewall typically blocks unsolicited traffic from reaching computers behind the firewall. How does it determine what's unsolicited? Modern firewalls use **stateful packet filtering** to determine what constitutes unsolicited traffic.

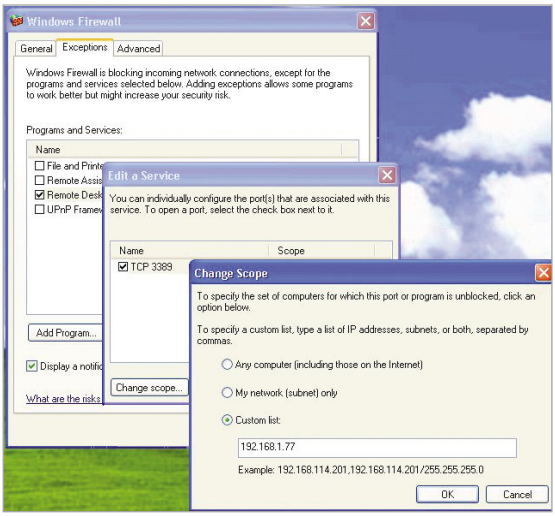
A firewall performing stateful packet filtering looks at the TCP/IP packets your computer sends out and remembers where they came from. It keeps track of this, and when a Web server sends you a page (again carried in TCP/IP packets), the firewall remembers your initial request and allows the packets through. Without stateful filtering, the firewall would reject these packets by default.

Stateful packet filtering is the key to keeping your computer invisible to the Internet. From the outside, no one would be aware that your computer is connected to the Internet, but when you desire, your computer can safely access the Internet.

Inbound & Outbound

Many firewalls filter traffic in one direction only: inbound to your computer. However, a new breed of firewalls tries to prevent spyware and viruses that have infected your computer from attacking other computers on the Internet. These firewalls also monitor your *outbound* traffic and only allow applications you authorize to access the Internet.

Bidirectional firewalls are great in theory, but in practice they suffer from two flaws. First, you have to grant each application access to the Internet. This can become tedious and prone to error.


Windows Firewall
General
Exceptions
Advanced
Windows Firewall is blocking incoming network connections, except for the programs and services selected below. Adding exceptions allows some programs to work better but might increase your security risk.
Programs and Services:
Name
File and Printe
Remote Assis
Remote Desk
UPnP Framew
Add Program...
Display a notific
What are the risks
Edit a Service
You can individually configure the port(s) that are associated with this service. To open a port, select the check box next to it.
Name
Scope
TCP 3389
Change scope...
Change Scope
To specify the set of computers for which this port or program is unblocked, click an option below.
To specify a custom list, type a list of IP addresses, subnets, or both, separated by commas.
Any computer (including those on the Internet)
My network (subnet) only
Custom list:
192.168.1.77
Example: 192.168.114.201,192.168.114.201/255.255.255.0
OK
Cancel

Creating an exception with Windows Firewall allows you to control who can access a service on your computer.

The second—and perhaps more important—flaw is that the firewalls really have no way of determining the authenticity of an application. If your computer becomes infected by a virus or spyware, such malware could masquerade as a legitimate application, fooling the firewall into granting it access to the Internet.

So, What *Do* Firewalls Deter?

Firewalls do not grant your computer complete immunity from security problems. As we've noted, a firewall simply controls what data is passed to your computer. A firewall alone may not defeat viruses, spyware, and other malware. (This is why we also have antivirus and antispyware applications.) However, firewalls do protect your computer from intruders on the Internet who can easily hijack an exposed computer running Windows, because most Windows computers have several ports open that a malicious intruder could use to attack and seize control of your system.

Deploying A Firewall

The first task in setting up a firewall is determining where to deploy it. If you have just one computer, protecting yourself with a firewall is much easier than if you have a network of computers to shield. With one computer, you can use either a software-based firewall that runs on your computer or a physical firewall that lies between your computer and the Internet.

Software-based firewalls such as ZoneAlarm (www.zonelabs.com) and the Windows Firewall bundled with Windows XP are more than adequate for most computer users protecting a single computer.

If you have a home network and want to protect all of your computers, you'll need a firewall that acts as a gateway for all of your computers. This can be a DSL (Digital Subscriber Line) router or cable modem with firewall functionality included, or it can be a dedicated firewall device.

An additional option is available for users with either Windows 2000 or Windows XP. Both of these operating systems offer a feature called ICS (Internet Connection Sharing) that allows a single computer to act as a firewall for a group of computers on a network. Each computer on the network would route all of its Internet traffic to this computer, and it would in turn protect the others from intruders.

We don't recommend this deployment model for several reasons. First, ICS doesn't offer as much protection to a network as a separate, physical firewall can. Using ICS also imposes a performance penalty on the computer acting as a firewall, depending upon how much traffic it's required to filter.

The optimal deployment scenario for most networks is a physical firewall device that sits between your Internet connection and your computers. Each computer is connected via a hub or switch, and configured to use the firewall as the default gateway. You can also use a software-based firewall in addition to a physical firewall as an added layer of security.

Installing A Third-Party Firewall

Although the firewall included with Windows XP adds a capable layer of protection to your computer, not everyone will be satisfied with its inability to control your applications as they attempt to access the Internet. One excellent alternative to consider is ZoneAlarm, available free from Zone Labs (www.zonelabs.com).

To install ZoneAlarm, download and then double-click the installer. Click Next, uncheck the two boxes that sign you up for Zone Labs product news, and click Next again. Accept the License Agreement, and click Install. After a few moments, the installer will finish, presenting you with a survey you can skip if you prefer. Click Finish, and when prompted, click Yes to start ZoneAlarm. Click Free ZoneAlarm in the License Wizard, then click Next and Finish.

The next step is configuring ZoneAlarm. When the Configuration Wizard launches, click Next, and select Yes under the Configure Internet Access To Allow Web Surfing. (We're assuming that you'd like access to the Web, of course.) Click Next and then Done. Click OK to restart your computer, and the ZoneAlarm installation will be complete. ZoneAlarm is enabled when your computer restarts, and displays a window with various security statistics. You can close this window, and when necessary, reopen it by clicking the ZoneAlarm icon in your System Tray. Remember that you can allow specific computers on your network access to your system by adjusting ZoneAlarm's firewall settings.

ZoneAlarm will warn you when various programs are attempting to access the Internet. The frequency of these warnings will decrease after the system has "learned" which applications are allowed access. ❙

Configuring Windows XP's Firewall

If you're using Windows XP and have updated your system to Service Pack 2, you have a preconfigured firewall already deployed on your computer. In a welcome change of philosophy, Microsoft has even configured the Windows Firewall to be turned on by default, despite the potential for confusion amongst users.

Out of the box, the Windows Firewall is a perfectly adequate firewall, blocking intrusion attempts with ease. Yet, as with many applications, a few tweaks can improve its performance.

First, launch the Windows Security Center. This is the central program for maintaining your computer's overall security. Click Start, Control Panel, and Security Center. If you haven't previously disabled the Windows Firewall, you should see a green On button next to the Firewall icon.

Next, click Windows Firewall under Manage Security Settings For. This will open the General tab of the Windows Firewall utility. The default setting for Windows Firewall is On (Recommended) with Don't Allow Exceptions unchecked. (An easy way to understand exceptions is to think of them as open ports. Each exception you create opens a port or doorway into your computer. By default, the Windows Firewall comes with four preconfigured exceptions, and one of the four exceptions enabled: Remote Assistance. Whenever possible, avoid creating exceptions.)

If you do need to create an exception, you can reduce your PC's potential exposure. For example, Remote Desktop is a convenient tool for administering a computer remotely, but you wouldn't want the entire Internet giving you a "helping" hand. To restrict who can access your computer via Remote Desktop, click the Exceptions tab, highlight Remote Desktop, and click the Edit button. This will open the Edit A Service window.

Next, click Change Scope. By default, any computer can connect to yours. Click the Custom List option and enter the IP address of the computer you want to allow to connect to your computer. Click OK.

Testing Your Firewall

Setting up a firewall is only the first step. Be sure to test to ensure that your firewall is doing its job. One of the easiest ways to verify that your firewall is working is to visit Shields Up! (www.grc.com). Shields Up! will probe your firewall in an attempt to illustrate any gaps in your protection.

Do I Really Need A Firewall?

Many people consider firewalls a nuisance—too much trouble to bother with. Browse the Internet and you'll hear stories from people who claim never to use a firewall (or antivirus software, for that matter) and yet have never had a problem.

Don't be one of those people. By default, Windows leaves ports open for networking purposes. Unless you're savvy enough to disable these ports, your computer is dangerously vulnerable when connected to the Internet. Tests have shown that an unprotected computer running Windows lasts about 10 minutes when connected to the Internet. After that, it's more than likely to have been successfully attacked, hijacked, and used to attack other unprotected computers.

It's not absolutely necessary to run a software-based firewall *and* a physical firewall, but the added protection wouldn't hurt. And it would certainly be foolhardy to decide not to use a firewall at all. Smart users realize that the Internet can be a hostile place and that implementing a firewall—inconvenient though it might be—is far easier than cleaning up the havoc an intruder can wreak upon your computer. RS

BY CHRIS JACKSON

Guard Duty

Choosing & Using Antivirus Protection On A Network

After installing a home network, the next step is protecting the PCs that connect to it. Part of that procedure requires implementing antivirus protection, but how you approach that protection can vary depending on your budget, your network size, your familiarity with network configurations, and the amount of time you're willing to devote to the process.

Protecting your network from viruses boils down to three methods. One of these involves using standalone antivirus programs on each PC connected to your network, while another involves using antivirus software specifically designed for networks. Yet another method blends benefits of both single-user and network-focused programs. Each method has its advantages and disadvantages.

Cheap But Effective

When installing antivirus protection on a single, non-networked PC, your choices are plenty and affordable. In addition to the wide selection of premium antivirus products available on the market, there are also several highly effective free options, including Grisoft's AVG Anti-Virus Free Edition (free.grisoft.com), Avira's AntiVir PersonalEdition Classic (www.free-av.com), and Alwil Software's Avast! 4 Home Edition (www.avast.com).

Most of these programs are for use only on single PCs and cannot be used to remotely configure and run antivirus protection on other PCs connected to a network, though they can be deployed on individual computers on the network. For example, you can provide antivirus protection for the computers on your network by installing individual copies of AVG Anti-Virus on each PC. While this method is free and effective, administration of the programs must be accomplished from each PC. If your kids use one of the PCs on the network, you'll need to regularly check the PC to ensure the resident protection of the antivirus program is active, that the program is successfully receiving virus definition updates, and that automatic (or manual) scans are accomplished. Unless you're willing to regularly monitor the PCs on your network—in person—to ensure the antivirus software is running as it should, you should consider antivirus products specifically designed for networks.

There is one exception to the in-person monitoring rule when it comes to single-user antivirus programs. Trend Micro's PC-cillin Internet Security 2006 ($90 for a three-user Home Security Pack) includes a centralized management console that allows antivirus administration for all PCs on the network. Although this feature isn't quite as robust as the network administration tools included with network-centric antivirus applications, it certainly gets the job done and can prove to be a perfect fit for most administrators of home networks.

Expensive But Expansive

Most developers of consumer antivirus software also offer network antivirus products that are primarily marketed toward businesses of all sizes. These products allow administrators to remotely install and manage the antivirus software on networked PCs, which differs from most single-user products, which must be managed from the PCs on which they reside.

Although these are business products, they can prove useful in certain home networks. If you have a home-based business, have several PCs connected to your network, and you're experienced in network administration, a network antivirus program might be a better option than a single-user antivirus program. These programs let you use a centralized location (such as your primary PC) to run virus scans on networked PCs and change configuration options remotely.

You can also use the network antivirus software to create installation CDs that include the exact configuration you want, and then use that CD

to install the software on computers that aren't connected to the network at all times. These programs also streamline the updating process, allowing you to download updates to your centralized location and then install them on networked PCs, in turn saving bandwidth across the network.

On the downside, these products are generally far more expensive than consumer-based antivirus programs, and the more computers on your network, the more you'll pay for protection. Further, network antivirus programs require much more configuration to get them up and running. For the software to effectively protect all computers on the network, it must run from a server, or a computer that's always running and uses Windows 2000, Windows XP Professional, or Windows Server 2003.

If you're not familiar with networking concepts, or if you don't have the time to handle the required extensive configuration, you're probably better off using single-user, consumer-based antivirus programs. But if you want the ultimate in antivirus protection and control, network antivirus is the way to go.

Although there are several choices for network antivirus, many are cost-prohibitive for the average consumer, particularly because they often require the purchase of at least five licenses. For example, the Symantec AntiVirus 10.1 Business Pack supports five users for $251, and McAfee Active VirusScan SMB Edition supports five users for $270. Not all network antivirus products require at least five licenses; Grisoft's AVG Network Edition is only $75 for two, two-year licenses.

Deploying PC-Cillin

There are 30-day evaluations available for both PC-cillin Internet Security 2006 and AVG Network Edition, so if you determine that free, single-user antivirus products aren't the right solution for your network, use the trials of these products to find which works best for your environment. Because PC-cillin is far easier to configure than AVG Network Edition, we recommend installing it first (you can download the evaluation from www.trendmicro.com /download/trial/trial-pcc.asp).

To use the network features of PC-cillin, you'll need to install the evaluation on each PC on your network, so it's a good idea to use separate email addresses to obtain the evaluation to avoid potential conflicts with duplicate registration keys on your network. After installing PC-cillin, open the program on your primary PC and click the Network Security button. Next, create a password that you'll use to access the network configuration, type it again to confirm it, and click OK. Next, click Private Network Connection, type your password, and click OK.

On the Private Network Connection screen, you can access the antivirus configuration of other PCs on your network. However, you'll first need to configure the Network Security portion of PC-cillin on those computers using the same password you used on your primary PC. After that, return to the Private Network Protection screen on your primary PC and click the Refresh button. The utility will scan your network for PCs using supported versions of PC-cillin, and if it finds any, it will list them with their computer name, local IP address, product version, and subscription status.

If the utility finds no computers, make sure the evaluation is installed on those PCs and they're all configured using the same password. If those PCs are using software firewalls, you'll likely need to instruct the firewalls to allow PC-cillin to access resources on the computers. When your networked PCs do appear in the Private Network Protection utility, click one of the PC listings, choose View Properties from the pulldown menu, and click Go. On this window, you'll see the local (primary PC) and remote (networked PC) versions of the program, virus scan patterns, and many other variables related to the PC-cillin Internet Suite. This window gives you an instant indication of whether the remote PC's program needs updated.

Clicking the Security tab on the Properties window reveals information about the remote PC's antivirus state, including time of last scan, time last virus was found, last virus found, last infected file, last scanned file, and last update. On the Logs tab, you can select a date from an on-screen calendar and view the log for that date. On the Settings tab, you can configure multiple antivirus settings for the remote computer. For example, you turn the following options on or off: real-time virus protection, incoming email scan, outgoing email scan, Web mail scan, and automatic update. To change any settings, simply click the button for the setting and click Apply.

Back on the Private Network Protection screen, select a networked PC, choose Scan from the pulldown menu, and click Go to perform a virus scan on that system. Although you can remotely instruct the PC to perform a scan, you must still physically access that PC to see the results of the scan and take any action. You can also update the virus definitions on the remote PC by selecting the computer, choosing Update, and clicking Go.

PC-cillin scans for other computers on your network that use the antivirus software, allowing you to remotely manage antivirus protection on those machines.

Deploying AVG Network

Unlike configuring single-user antivirus programs, setting up software such as AVG Network Edition is a complex, tedious process. If you're not familiar with network configuration, or if you don't plan on running your primary PC as a server, you should instead protect your network using single-user AV software. However, if you have many PCs and need thorough control over your antivirus environment, a product such as AVG Network Edition could be a better choice.

Although the full configuration of AVG Network Edition is too complex to define in this article, it helps to understand the concepts behind such a program. The most difficult portion of configuring network antivirus software is enabling remote administration, because the software assumes that you're using a dedicated server along with clients on your network.

Several modules comprise the architecture of AVG's remote administration scheme. The AVG DataCenter includes a communication database and the AVG TCP Server, which enables communication between AVGADMIN and clients (the remote computers), where AVGADMIN is a program that enables network installation, administration, and updating of the clients. Finally, the Grisoft server provides the AVG TCP Server with update files. For more information on how to configure this software on a network, visit www.grisoft.com/doc/downloaddoc/lng/us/tpl/tpl01 and download the AVG Network Edition Step-by-Step Guide, as well as the AVG 7.1 Remote Administration Introduction, Quick Guide, User Manual, and Reference Guide.

Make A Smart Choice

Preventing viruses from infecting your network is always a top priority. Some users tend to feel their networks are protected as long as there's antivirus protection only on the computer that's physically connected to the network. Unfortunately, any PCs connected to the network can contract viruses, which in turn can infect other PCs.

How you approach your network's antivirus protection depends on numerous factors. If you're using your network for non-business purposes and have only two or three computers on the network, using free, single-user antivirus products is an effective solution. However, that choice requires that you regularly check the networked computers to ensure the antivirus software is running and updated, and if you don't schedule automatic scans (or if a user turns off those scans when they run), you'll need to access the PC to perform them.

This is where a hybrid product such as PC-cillin Internet Security 2006 becomes handy, because you can perform scans and updates and even change configuration options for networked computers all from your primary PC. On the other hand, if you have experience in network configuration and use one of your networked PCs as a server, a network AV product can deliver more control over your environment.

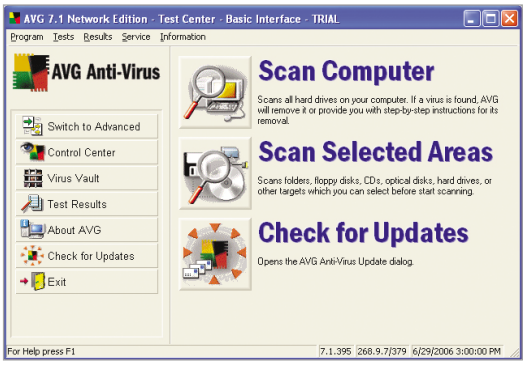
Be sure to make an antivirus choice before installing your network, because you shouldn't use your network without proper protection. If you have your antivirus programs ready to go before you build, you can immediately install and configure them and prevent further delays in actually using your network. RS

BY CHRISTIAN PERRY

Weighing Antivirus Pros & Cons

When looking to protect your network from viruses, you can take one of three routes: single-user antivirus, network antivirus, or a hybrid (specifically, PC-cillin Internet Security 2006). The following chart details major differences between these products.

	Single-user antivirus	Network antivirus	Hybrid (PC-cillin)
Cost	Cheap—many free programs are available	Mostly expensive ($250 and up), though some affordable options exist	Relatively cheap ($90 for three users)
Remote installation	No	Yes	No
Remote scanning	No	Yes	Yes, but must access remote PC for results
Remote updating	No	Yes	Yes
Remote configuration	No	Yes	Yes, but limited
Remote tracking	No	Yes	Yes
Remote scheduling	No	Yes	No
Remote log access	No	Yes	Yes


AVG 7.1 Network Edition - Test Center - Basic Interface - TRIAL
Program Tests Results Service Information
AVG Anti-Virus
Switch to Advanced
Control Center
Virus Vault
Test Results
About AVG
Check for Updates
Exit
Scan Computer
Scans all hard drives on your computer. If a virus is found, AVG will remove it or provide you with step-by-step instructions for its removal.
Scan Selected Areas
Scans folders, floppy disks, CDs, optical disks, hard drives, or other targets which you can select before start scanning.
Check for Updates
Opens the AVG Anti-Virus Update dialog.
For Help press F1
7.1.395 268.9.7/379 6/29/2006 3:00:00 PM

Although AVG Network Edition looks as simple as the program's free version, it requires intricate configuration to get up and running across the network.

Protect Your PC With Passwords

Hackers Prey On Computers Without Password Barriers

Passwords can be annoying, time-consuming to use, and sometimes even forgettable. Unfortunately, passwords are essential for securing PCs, especially those with dedicated Internet connections. Without password barriers, an intruder who gets past your other defenses may be able to enter your network device's settings and lower your security preferences. It would be as if you installed a security system in your house and left the door open.

Your Security Is Important

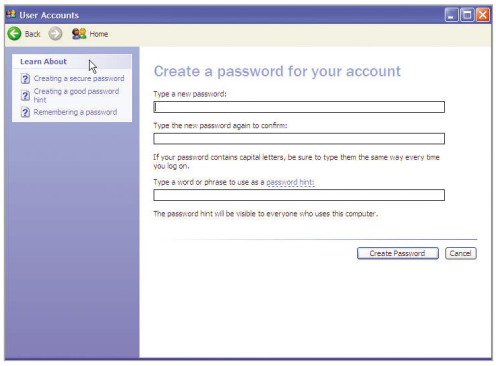
All user accounts, especially the administrator, should employ a password to keep out intruders. On a wireless network, put a password on your network router or access point to prevent unauthorized users from changing your WEP, WPA, or MAC security settings. Make sure you change the default password on your network device because anyone can get the default settings from the manual or the manufacturer's Web site. For example, on a Linksys router the default logon has no username and the password is "admin."

Steps To Password Protect

Windows logon passwords don't take long to set up and they should be enough to keep out minimally skilled intruders. To create a password for accounts on your computer in Windows XP, open Control Panel and double-click User Accounts. Select an account and click Create My Password. Enter your new password into the Type a New Password field. A password is case sensitive so you'll need to remember if you've entered special characters or capital letters. Type the same password into the Type The New Password Again To Confirm field. In WinXP, you are allowed to type a phrase or word to help you remember your password, but any phrase you enter should be a clue that only you will recognize. Click Create Password to apply your password. Remember, all user accounts should have a password.

To create a password in Windows 2000, open Control Panel and double-click Users and Passwords. Click the checkbox for Users Must Enter A User Name And Password To Use This Computer. In WinXP, a password is automatically applied when you create a password, but in Win2000 you need to click the Users Must Enter option to force users to logon the PC. Select a User Name and click the Set Password button under Password For [User Name You Selected]. Enter a password in the New Password field, and then enter it again in the Confirm New Password field. Click Apply to set the password for that username.

Your network router or access point password should be easy to set as long as you can reference your users guide. Open your Web browser and type in the default IP (Internet Protocol) address for your router or access point. The default IP address can be found in your users guide, and will look similar to http://192.168.1.1. You will be prompted to enter your username and password; again, reference the users guide or check the manufacturer's Web site. Enter the default username and password to access your networks settings. Locate where you can Change Your Password and enter your new password. As with your Windows' logon password you'll probably have to do this twice. Save your settings and close the browser. You will now have to enter this password when you want to access the network device settings.


User Accounts
Back
Home
Learn About
Creating a secure password
Creating a good password
Remembering a password
Create a password for your account
Type a new password:
Type the new password again to confirm:
If your password contains capital letters, be sure to type them the same way every time you log on.
Type a word or phrase to use as a password hint:
The password hint will be visible to everyone who uses this computer.
Create Password
Cancel

You can change or create user account passwords by double-clicking User Accounts in your Control Panel.

Practical Password Practices

The passwords on your PC and network device should be different from ones you use for Internet banking or email. Don't use single words in the dictionary because they are easy to randomly generate. Finally, it's a good idea to write down your passwords, but don't put the written copy somewhere visible. Keep it hidden in a place where only you can find it. RS

BY NATHAN LAKE

Setting Up WEP For Wireless Networks

Shore Up Your Wireless Defenses

Do you feel a little nervous when the neighborhood kid wears his "I read your email" T-shirt? If you have an unprotected home network, you should take that kid more seriously. Whether your network has valuable information or not, malicious users want to break into it. Even if you don't store your passwords on your hard drive (you don't do that, right?), hackers want to take over your computers. Some of them will just mooch your broadband Internet access, some will rifle through your personal documents, and some will use your machines to attack others. Although you've protected your network by installing a router that has a built-in firewall, you'll open the network to attacks again when you take it wireless—unless you put a new defense in place. That defense is wireless transmission encryption.

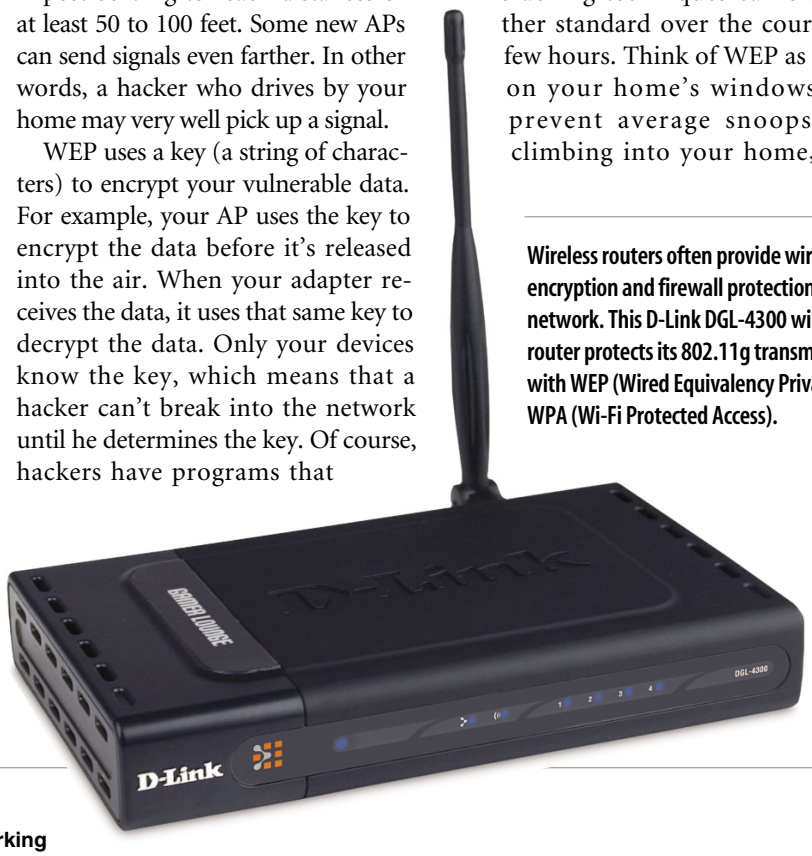
Because encryption is so important to network security, manufacturers build it into many wireless routers and APs (access points). Two popular encryption standards are WEP (Wired Equivalency Privacy) and WPA (Wi-Fi Protected Access); your AP may support one or the other, or both. We'll show you how to set up the older (but still serviceable) WEP encryption. If you're interested in WPA encryption and its successor, WPA2, check out the article "WPA Is A-OK" on page 118. It's worth noting that wireless adapters that don't support your AP's encryption standard (WEP or WPA) can't connect to your network. If you buy a new AP for an old network, you may need to upgrade some components to take advantage of the AP's best encryption.

WEP

When data flows between your AP and your notebook's wireless adapter, it's vulnerable. A hacker who is within your AP's range can intercept this data and, if it's unencrypted, view it. The encryption protects the data during its flight. And although you probably don't wander much further from your house than the backyard when you're using your notebook, your AP's range may extend well beyond that distance. Expect 802.11g to reach distances of at least 50 to 100 feet. Some new APs can send signals even farther. In other words, a hacker who drives by your home may very well pick up a signal.

WEP uses a key (a string of characters) to encrypt your vulnerable data. For example, your AP uses the key to encrypt the data before it's released into the air. When your adapter receives the data, it uses that same key to decrypt the data. Only your devices know the key, which means that a hacker can't break into the network until he determines the key. Of course, hackers have programs that attempt to crack the key, which is why you'll want to change your key on a regular basis. If you set a key when you first install your AP and then ignore it, you're ensuring that any hacker who manages to crack the key has access for an unlimited amount of time.

When you enable WEP for your network, you can most likely choose between 64-bit and 128-bit encryption. The key makes up 40 and 104 bits, respectively, and each key has a 24-bit code (hence 64-bit and 128-bit encryption). Choose the latter to provide the strongest defense. That said, you can't expect 128-bit strength to completely protect you, as some cracking techniques can crack either standard over the course of a few hours. Think of WEP as latches on your home's windows: they prevent average snoops from climbing into your home, but a



Wireless routers often provide wireless encryption and firewall protection for your network. This D-Link DGL-4300 wireless router protects its 802.11g transmissions with WEP (Wired Equivalency Privacy) or WPA (Wi-Fi Protected Access).

skilled criminal is going to find a way to enter your house.

Keep in mind that WEP encryption may slow your network a little. If you find that 128-bit encryption has a large impact on network performance you may need to back down to 64-bit encryption.

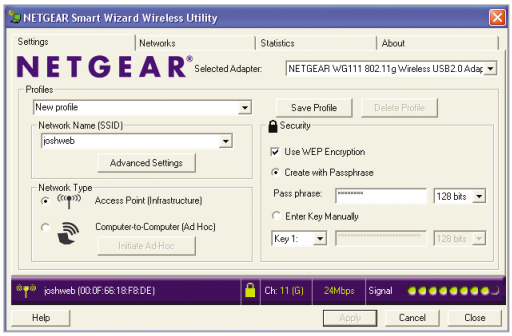
To determine whether you are attempting to connect to a WEP-protected network, check your PC wireless adapter's network utility or open Windows' Wireless Network Connection feature (you'll find the icon in your System Tray when your wireless adapter is active). The Windows Wireless Network Connection lists available networks and uses a lock symbol to indicate protected networks, but it doesn't indicate whether the encryption standard you are facing is WEP or WPA.

Set Up WEP

You can set up your network's encryption when you first install an AP or router, as well as any time after you've completed the network. Keep in mind that as soon as you enable WEP encryption, your PCs and notebooks no longer communicate with your network; you'll need to supply the key for each device so it can reenter the network.

The AP's (or router's) configuration menu houses your wireless encryption options. Browse your manual to find the device's IP address (such as 192.168.1.245) and then enter the address in your Internet browser. The configuration menu varies by device and manufacturer, but you probably won't have much trouble finding the section that handles wireless security; the configuration menus generally aren't very complicated.

You may need to create your own key. To do this, simply enter random numbers and letters into the appropriate field: letters between A and F, and numbers between 0 and 9. If you use 64-bit encryption, enter 10 characters; if you choose 128-bit encryption, enter 26 characters.



Type the network's WEP (Wired Equivalency Privacy) key into your adapter's network utility. Note that if your AP (access point) isn't broadcasting its SSID (Service Set Identifier), you'll need to enter the SSID into the utility. Otherwise, it will appear automatically.

Many of the configuration menus let you enter a passphrase that you can more easily remember. The menu then generates a key based on your password. You can use the password in lieu of the key on other devices from the same manufacturer, but devices from other manufacturers may not support passphrases, so be sure to write down the key, even if you use the pass-phrase feature. In our experience, you can use your passphrase to generate an identical key (to your AP's key) even with adapters from other manufacturers.

The configuration menu may offer up to four key fields, but you'll only need to enter one key. If you enter a different key into each field, you'll find that three of the keys are inactive. Some vendors add those extra fields so you can save time when you come back later to enter a new key: You can simply select one of the other three keys, rather than enter a new key.

If you choose a password for Passphrase field in your AP's (access point's) configuration menu, it will automatically generate your WEP (Wired Equivalency Privacy) encryption key.

Connect To Your Network

Once you enable WEP via your router or AP, you can reconnect the network's computers to the network. If you want to use Windows' Wireless Network Connection feature, right-click its icon in your System Tray and then click View Available Wireless Networks. The feature displays any networks that your adapter can reach—you may find many nearby networks if you live in a crowded area. Select your network from the list and then click Connect. Next, you'll need to supply the WEP key. The feature then lets your computer connect to the WEP-encrypted network.

Many adapters include their own wireless networking utilities. If you open your adapter's utility, you may see a message that asks permission to disable Windows' Wireless Network Connection. Disable the feature and then use the adapter's utility to select your network. Enter the wireless key (or passphrase, if the utility supports it). Finally, open your browser (or your Network Connections folder) to make certain you can access the network.

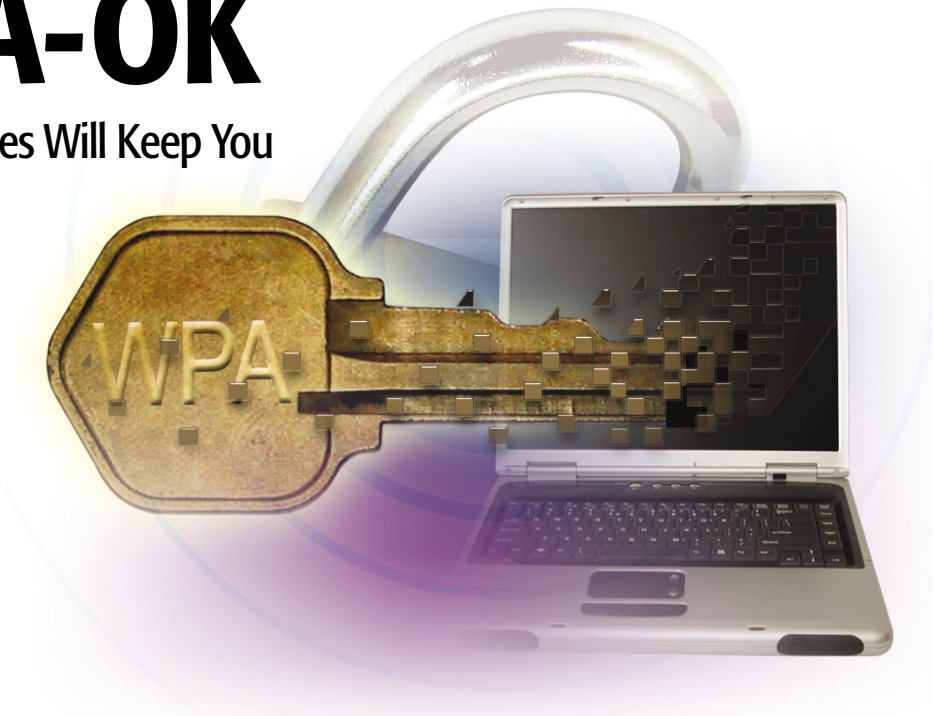
Don't Drop Your Guard

If all of your network's equipment also supports WPA or WPA2, don't bother with the weaker WEP standard. That said, if WEP is your only option, don't overlook it. Without encryption, you're waving a white flag to any remotely-tech-savvy snoop who drives by (or lives near) your house. RS

BY JOSHUA GULICK

WPA Is A-OK

WPA & WPA2 Security Modes Will Keep You Well-Protected



If you walk in on a conversation between two network administrators, don't be surprised if it seems like they're speaking in a foreign language. TKIP, RADIUS, SSID, WLAN, DHCP WEP, WPA—there are so many acronyms that deal with networking that learning them seems like an impossible mission. Though knowledge of all the letters, numbers, and technologies will help you set up a high-performance network, the most important acronyms to learn are those that can help keep your network as safe as possible. As technology advances, so do resources for hackers. Networks that were considered safe only a year or two ago can be easily cracked by a good hacker. WPA (Wi-Fi Protected Access) offers an easy way to keep your network secure. Let's take a look at WPA security and how it can help your network stay safe.

A History Of WPA

WPA made its first appearance as a wireless security option in 2003. It was designed to be a step above WEP (Wired Equivalent Privacy), the original standard in wireless network security. As the name suggests, WEP-protected networks were supposed to be just as safe as LANs (local-area networks), yet users would have the freedom offered by wireless devices. This safety came through its encryption key. However, there were serious flaws found in **WEP algorithms** (the formulas that generate security codes), and the short security IVs (initialization vectors) buckled when hackers attempted to crack WEP-secured systems. Even though it isn't the safest solution available, WEP can still serve a purpose on your wireless network. For more on WEP, see Setting Up WEP For Wireless Networks on page 116.

WPA was designed as a temporary solution to WEP. Though work was underway on WPA2 (also known as 802.11i), the vulnerabilities that were uncovered in WEP needed to be addressed immediately. That's how we got WPA. It uses the same RC4 stream cipher encryption that was employed by WEP, but there are some changes that make it a better security option. The major change is that while WEP employed a static or unchanging key, which allowed hackers more than enough time to study IVs and crack the WEP code, WPA uses TKIP (Temporal Key Integrity Output) which mixes the IV with the security key instead of just adding it on to the end of the security key as was the case with WEP. TKIP also features a rekeying mechanism, which lets the user set a time interval at which the key changes.

The successor to WPA, WPA2, was ratified in June 2004. Much like WPA, WPA2 still uses a mechanism for dynamic key generation to keep hackers from locking on to your security settings, but there is a major difference. While WPA uses the old RC4 cipher to generate security keys, WPA2 uses AES (Advanced Encryption Standard), a much safer block cipher, for encryption. It also works much better for enterprises that use an authentication server for user access.

Let's Get Wireless

As confusing as networking acronyms and terms can be, we found setting up WPA security on our wireless network surprisingly easy. Since WPA made its debut in 2003, nearly all wireless routers, including the Linksys WRT54GS we used, and WAPs (wireless access points) currently on the market are equipped with WPA capability. Many also have WPA2 capability either out of the box or as a firmware upgrade.

Before you even get the router or WAP out of its packaging, go to

Microsoft's Download Center (support.microsoft.com) and get update KB893357. This download will enable Windows XP to support WPA2.

The physical installation of a wireless router in a wireless home network is straightforward. It usually consists of running an Ethernet cable from your modem to a marked port on your router and then running another Ethernet cable from one Ethernet port to the administrative computer, or the computer that you want to use to manage the settings of your router and your wireless network.

No matter what type of wireless network you set up, it's always a smart idea to change the network name and, of course, the password from the default. Even if you don't change the password right away, change the network name: Hackers know the default names and default passwords for most wireless routers. For instance, by default, our Linksys router set up a network named Linksys. If a hacker sees this, he knows that the user might not have changed the default password, which he also knows, giving him easy access to the information of any computer on the wireless network.

After you get your router hooked up to the administrative computer, go to the Web site suggested in its user manual to continue set up. The Web site will vary with the brand of router. For instance, a Netgear WGR614 router tells you to go to www.routerlogin.net/basicsetting.htm to configure your router, while the Linksys WRT54GS instructs you to go to http://192.168.1.1 to continue configuration.

Once you access your router's configuration Web site, set up your security preferences. You'll most likely have a few security modes to choose from, such as WEP, WPA Personal, WPA Enterprise, WPA2 Personal, or WPA2 Enterprise when you're setting up your network preferences. WPA Personal and WPA2 Personal versions use a PSK (pre-shared key) security access mode. A PSK is basically just a password that users have to know to log onto a network. Users who take advantage of Enterprise modes will generally employ a server to regulate network access. As the name suggests it was designed as a security option for larger networks used by big businesses.WPA2 is a backward-compatible technology, so even if you have a wireless card that was only designed to support WPA security, you'll still be able to log onto a WPA2-secured network. Some of these WPA devices can be upgraded to implement WPA2 security via firmware upgrades; however, because WPA2 is so computationally intensive, some hardware will have to be replaced. Check manufacturers' Web sites for firmware upgrades.

If you have a basic wireless network secured by a WEP, you'll probably be safe. Any hacker with the time and resources to crack a WEP security protocol probably has bigger fish to fry than stealing digital pictures of your family's Christmas. However, even though you may be able to get by with WEP security, there are better solutions available, namely WPA and WPA2. WPA can serve as a more secure alternative on most access points and wireless routers because it features a security protocol that is much tougher to crack than a WEP. Its successor, WPA2, which utilizes a more secure algorithm and keying process, is now available on numerous wireless routers and access points today, and is backward compatible, so even if your hardware might not support WPA2, you can still run WPA or WEP until you upgrade your hardware. Bottom line, even if you aren't fluent in network-speak, you can still set up the WPA security mode very easily, and the reward of having a safe wireless network is well worth the few minutes you'll invest doing so. RS

BY SAM EVANS

Wireless Security Glossary

Here are a few terms that you might come across as you try to update your WEP network to a WPA- or WPA2-secured network.

802.1x. This is an authentication standard used especially in WPA Enterprise and WPA2 Enterprise networks that authenticate users requesting access to a network.

AES (Advanced Encryption Standard). This block cipher encryption standard is the basis for WPA2. It is stronger than the RC4 stream cipher and is on the cutting edge as far as wireless security goes.

PSK (Pre-Shared Key). PSK mode, sometimes referred to as personal mode, is generally the mode in which most home networks will function. In this mode, the network administrator will simply create a password that computers within range must enter to get network access.

RADIUS (Remote Authentication Dial-In User Service). This security system is employed by medium-sized to large businesses and ISPs (Internet service providers). It requires users to enter a username and password to access a network. This information gets passed to a dedicated RADIUS server which checks the information and, if the information is authorized, gives users network access.

TKIP (Temporal Key Integrity Protocol). This security protocol (pronounced tee-kip) was introduced with WPA. It featured key mixing, which made it considerably more difficult to crack than WEP. With WEP a traffic key was formed by linking a key with an IV. TKIP improved upon this by hashing the WPA key with an IV. ❙

MAC-Based Security For Wireless Networks

Secure Your Wireless Network With MAC Address Filtering

Wireless networks are incredibly convenient: no wires to clutter up your home, the freedom to roam with your notebook outside, the ability to add additional computers to your network without being limited by the number of physical network ports. However, with this convenience comes the burden of maintaining the security of your wireless network. One strategy has been to use MAC (Media Access Control) address filtering. We'll show you how to implement MAC address filtering and explain when to use it.

What Is A MAC Address?

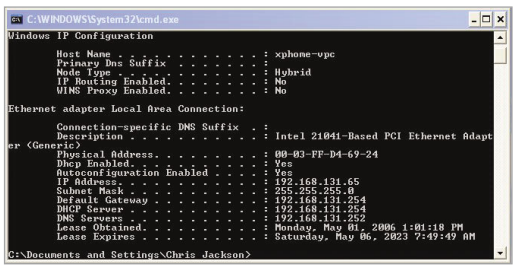
One way to think of a MAC address is as a sort of serial number for your computer's network card or interface. When a company builds a wireless NIC (network interface card), it encodes a unique MAC address into the firmware of the card.

MAC addresses are written in hexadecimal notation, and there are over 281 trillion possible addresses. Most implementations denote the MAC address in six groups of two hexadecimal digits, such as this: 00-03-FF-D4-69-24.

MAC addresses are used so that network devices know how to communicate. When a computer on a network wants to communicate with another computer or network device, it needs to determine the MAC (sometimes referred to as the hardware address) of the recipient device.

Wireless Security: A Primer

Wireless networks need to have some form of security, lest strangers eavesdrop on your network traffic or piggyback on your Internet connection. Security comes in two forms: **authentication** (determining who is granted permission to use your wireless access point) and **confidentiality** (so that no one can read your network traffic). The main methods of providing these two security components for home wireless networks are WEP (Wired Equivalent Privacy) and WPA (Wi-Fi Protected Access).


C:\WINDOWS\system32\cmd.exe
Windows IP Configuration
Host Name . . . . . : xphome-vpc
Primary Dns Suffix . . . . . :
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No
Ethernet adapter Local Area Connection:
Connection-specific DNS Suffix . :
Description . . . . . : Intel 21041-Based PCI Ethernet Adapter (Generic)
Physical Address. . . . . : 00-03-FF-D4-69-24
Dhcp Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
IP Address. . . . . : 192.168.131.65
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.131.254
DHCP Server . . . . . : 192.168.131.254
DNS Servers . . . . . : 192.168.131.252
Lease Obtained. . . . . : Monday, May 01, 2006 1:01:18 PM
Lease Expires . . . . . : Saturday, May 06, 2023 7:49:49 AM
C:\Documents and Settings\Chris Jackson>

In addition to providing you with information about your NIC's IP settings, the Ipconfig command also displays the MAC address of your NIC.

WEP's Weakness

When vendors were first developing standards for consumer wireless equipment, WEP seemed to be the easiest solution to implement. WEP required a shared key that was encrypted and then sent to the wireless access point from a computer with a wireless NIC. Once the wireless access point accepted the key, both computer and access point encrypted all the traffic between the two devices. Initially the system seemed robust enough to prevent any attempts to break the encryption process. It was also relatively easy for consumers to implement; all they had to do was create and copy an encryption key to each computer that wanted to access the wireless network.

However, there were fatal design flaws in WEP that eventually led to its demise. Hackers can crack or gain access to any WEP-protected wireless access point with easily obtained tools, and also listen in to any traffic that traverses the access point.

MAC Address Filtering

As an added layer of security for wireless networks, vendors added the ability to restrict access to specific MAC addresses. Since each wireless NIC has a unique MAC address, configuring this

Determining Your MAC Address

The MAC address of your NIC is stored in the firmware of the card itself. You can't access this directly, but Windows can help you. When Windows starts up, it loads software drivers that allow it to communicate with your NIC. These drivers tell Windows the MAC address of your NIC (amongst other information) and Windows stores the MAC address in its Registry. When Windows needs to send data across the network, it retrieves this address from within the Registry and uses the address to send the data on its way.

Fortunately, you don't have to dive into the nether regions of the Registry to retrieve your NIC's MAC address; let the ipconfig command do the heavy lifting for you. First, click Start and then Run. Enter **cmd** and click OK. This will open a command prompt where you can start programs simply by typing their names.

Next, type **ipconfig /all** at the command prompt and press ENTER. You'll see an assortment of information, but what you'll want to look for is a line listing Physical Address. At the end of this line is your NIC's MAC address. Be careful though, because there may be more than one NIC in your computer (usually a more traditional Ethernet adapter); be sure that you're reading the address of your wireless NIC and not the address of a regular Ethernet card.

WPA: The Sheriff Protecting Your Wireless Access Point

Although WEP has been touted by wireless vendors as an acceptable method of protecting access to your wireless network, the truth is that it's easily circumvented with simple tools that are freely available across the Internet. It doesn't take a computer scientist to break into your wireless network; with a few mouse-clicks, a miscreant can both monitor your traffic and use your bandwidth at will.

Fortunately, a new standard has become widely implemented within the last year. **WPA**, or Wi-Fi Protected Access, has proven to be a robust way to control access to a wireless network, as well as protect the traffic from eavesdroppers. Check to see if your existing wireless hardware supports WPA; if not, you'll be forced to rely upon WEP for protection. And if you're in the market for new wireless equipment, be sure it supports either WPA or the latest version, WPA2. ❙

layer of security was as simple as adding the MAC address (see our "Determining Your MAC Address" sidebar) of your computer's wireless NIC to your wireless access point's list of approved MACs.

When a computer attempted to authenticate to your access point, the access point would compare the MAC address of that computer's NIC with its list of approved MACs. If there was a match, great; authentication was successful. If the computer's MAC address was not listed, then the computer was denied access. In theory, this system was perfectly adequate for controlling access to small home networks with a few computers using the wireless access point.

Is Your Computer's MAC Address Truly Unique?

Unfortunately, the basic concept of restricting access based upon MAC addressing is fundamentally flawed: In most operating systems, spoofing a MAC address is not difficult.

Imagine a nightclub with a beefy bouncer at the door. He has a list of approved guests, and when a couple wants to enter they tell their names to the bouncer. But the bouncer is hard of hearing, and repeats their names to be sure he heard them properly. In addition, the bouncer has a very short-term memory. After perusing his list of favored guests, he opens the door and ushers them inside.

The next couple in line doesn't have a reservation, but they're desperate to get in so they try to scam our forgetful bouncer: They repeat the name they've just overheard from the previous couple. The bouncer scans his list of guests and sees that this couple's name is indeed on the approved guest list. Like the previous legitimate couple, these grifters are able to enter the swanky nightclub with ease.

Impersonating another MAC address is simple for most crackers. Relying on MAC addressing alone to protect your wireless network is foolhardy when the neighbor next door can download tools that will easily fool your digital "bouncer."

Making Do With What's On Hand

Unfortunately, many wireless access points and NICs don't support any security protocols other than WEP and MAC filtering. Although the price of wireless equipment has plummeted since its introduction, not everyone can afford to replace their wireless gear with newer equipment that supports WPA. In this case, using WEP with MAC filtering is much better than nothing.

Why? Although we previously said that reliance on these two methodologies is foolhardy, it's important to measure the threat. If you're stuck with WEP/MAC equipment, you can't protect yourself from a determined cracker. But you can utilize the two together to prevent the casual intruder from accessing your network, such as a neighbor who knows enough to spot an unprotected network but not enough to spoof a MAC address.

And an unfortunate truth is also on your side. There are many completely unprotected wireless networks out there. When presented with the choice of breaking into a WEP/MAC protected network or simply accessing a wide open access point, most crackers will save time and use the latter. RS

BY CHRIS JACKSON

Advanced Wireless Security Options

Protection For SOHO Wireless Networks

Although today's wireless home networks are convenient and easy to install, they are far less secure than old-fashioned wired networks. Out of the box, most wireless network are not protected—neighbors and passersby can easily tune into your wireless AP (access point) and sneak on to the Internet. With a bit of knowledge and some software, they can also eavesdrop on your wireless transmissions.

The default settings of most wireless APs offer little protection from freeloaders who want to use your network's Internet connection. And the default settings usually don't prevent the ability of hackers to uncover private information or access your computer to send out spam or viruses.

We'll address the advanced security options you can use to secure your SOHO (small office/home office) wireless network. First, we examine the typical built-in protections provided by wireless APs. Then, we discuss how to activate three additional technologies on your network for a more secure multilayer defense.

Built-In Protections

In addition to the obvious preventive measures you should use to protect your networked computers and devices (firewall software, antivirus software, regular backups, and updating your operating system), wireless networks need further security. This is largely because wireless devices communicate with radio frequencies, and hackers can easily intercept transmissions. The wireless AP is the core of your wireless network, and it offers some inherent features that protect wireless network communications.

NAT. Virtually all wireless APs include a feature known as NAT (Network Address Translator) technology. NAT effectively hides the computers attached to your network from hackers who might try to attack your system through the Internet. To do this, NAT uses a public IP (Internet Protocol) address for communications via the Internet, and it translates the public IP into private IP addresses for each of the computers or other wireless devices attached to your wireless network. NAT technology prevents outsiders from detecting the IP addresses of your wireless devices.

SPI firewall. Even if your individual devices or computers are running a software-based firewall, such as Windows Firewall in Windows XP, your wireless AP can add another layer of protection with its built-in firewall. Typically, wireless APs offer an SPI (stateful packet inspection) firewall that checks each **packet** (a block of network data) of incoming information to make sure it corresponds to an outgoing request from your computer. If the firewall does not recognize the source of an incoming request, it protects your system by discarding the request.

Administration tool. You administer wireless AP settings through a software interface, usually accessed with a Web browser from the computer that connects to the wireless AP. Most administration tools come with a default password set by the manufacturer. These passwords are widely known, so it's a good idea to change your wireless AP password. Additionally, some wireless APs include a remote administration feature that lets you access the tool from a remote computer. If your wireless AP offers remote administration, make sure it is disabled if you don't need it.

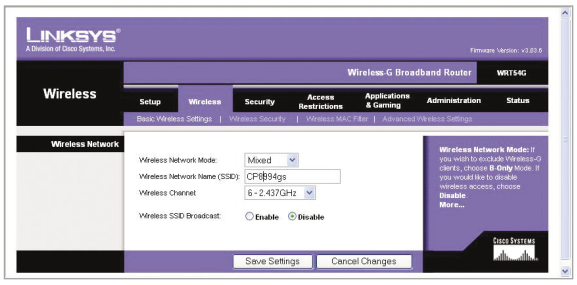
More layers. The built-in protections offered by wireless APs are not enough to completely secure your network. Additional layers of security

include changing the SSID (Service Set Identifier) name, keeping the SSID name private, filtering MAC (Media Access Control) addresses, and configuring encryption and authentication methods. Even if you use a wireless AP configuration wizard, double-check the following items to ensure your wireless network is protected.

SSID

The **SSID** is a one- to 32-character name for a wireless AP. It serves as an identifier so that wireless devices can differentiate among APs they detect. Wireless AP manufacturers provide a default SSID; for example, Linksys products ship with an SSID of "Linksys" and D-Link uses "WLAN." These default names are well-known to the hacker community. In addition, most wireless APs are set to broadcast their SSIDs so that wireless devices can find them. Of course, any wireless device within range of the AP (including neighbors and hackers) can find the SSID when it is broadcast.

To enhance security, you can make two changes to the default SSID information. The first change is to define a more secure SSID name. Secondly, you can change the wireless AP to stop broadcasting its SSID. Although sophisticated hackers can use techniques such as packet-sniffing tools to detect the SSID within transmitted messages, doing so takes significantly more effort than when your wireless AP broadcasts its SSID.



Changing the SSID (Service Set Identifier) configuration in the wireless AP (access point) configuration tool makes detecting your network more difficult for hackers and bypassers.

Change the SSID name. The wireless AP administration tool should include an option to redefine the SSID name. As noted previously, the name can be as many as 32 alphanumeric characters. Additionally, the SSID is case sensitive. Create an SSID as you would a strong password and avoid using names, words, or dates. Instead, use upper- and lowercase letters along with numbers, with a length of at least eight characters.

Disable the SSID broadcast. Before you disable the SSID broadcast, change any wireless devices to use the new SSID name. For most devices, you can access the SSID information by right-clicking the wireless connection and clicking Properties. Next, go to the computer that accesses the wireless AP administration tool and disable the SSID broadcast. Save the configuration change and test your devices to ensure they can connect to the wireless network. Because you changed the devices to connect to the new SSID, they will detect the wireless AP with the broadcast feature turned off.

MAC Address

A **MAC address** is a unique identifier for every device in a network. A permanent address, it consists of 48 bits (12 hexadecimal digits) normally assigned by the manufacturer. Using the MAC addresses of your wireless devices, you can restrict access to the wireless AP to only known devices. This method of access control is known as **MAC address filtering**.

If you administer a large wireless network or have many wireless devices coming and going, MAC address filtering is difficult to administer and not very effective. In addition, as with other security measures, MAC address filtering is not foolproof. Hackers can use wireless network analyzer tools to detect the list of MAC addresses. They can also use software to spoof the MAC address of an authorized device. However, if you have a small network, MAC address filtering is another layer of defense for hackers to defeat when used in combination with other security techniques.

Obtain MAC addresses. To learn the MAC address of a Windows 2000/XP notebook or desktop PC wireless adapter, go to the command (C:) prompt, type **ipconfig /all**, and press ENTER. In the information that displays, look for the Physical Address in hexadecimal format, for example, 00-03-47-35-5A-16. For Windows 95/98/Me computers, click Start, click Run, type **winipcfg**, and press ENTER. In the IP Configuration dialog box, select the network adapter and note the information in the Adapter Address (MAC address). For other types of devices, such as a PDA (personal digital assistant), check the product documentation to find out how to obtain the MAC address.

Configure and test. In the wireless AP administration tool, locate the MAC address filtering option. Enable this feature and enter the MAC addresses of the devices you want to permit on your wireless network. After saving the settings, test access with the permitted wireless devices. If possible, try to access the wireless network with a device that is not on the permitted MAC address list to ensure that nonauthorized devices are denied access.

Authentication & Encryption

Securing a wireless network requires authentication and encryption technologies. **Authentication** is the process of ensuring that a user is authorized to access the wireless network. For personal networks, authentication is usually handled with a username and password. In the corporate environment, authentication technologies include digital certificates, smart cards, and biometric information, such as a fingerprint.

Encryption makes information traveling over the wireless network unreadable to anyone who is eavesdropping on the transmission. Encryption algorithms (formulas) convert plain text into cipher text. Different encryption algorithms provide different levels of security.

Wireless authentication and encryption technologies. The original 802.11 Wi-Fi specification included **WEP** (**Wired Equivalent Privacy**) technology to address authentication and encryption requirements. However, the security provided by WEP proved insufficient. For example, the WEP encryption key, which defines the translation of plain text into cipher text, is static and does not change. By collecting a network's transmissions and using WEP-cracking tools, hackers can determine the encryption key and decode the information.

As a result of the security problems in WEP, the Wi-Fi industry began developing the more secure IEEE 802.11i standard. Until the new standard was finalized, however, the industry adopted **WPA** (**Wi-Fi Protected Access**) as an interim solution. WPA contains many improvements and addresses most of the security issues found in WEP.

The 802.11i standard, also known as **WPA2** (Wi-Fi Protected Access 2), was released in 2004 and is available on newer wireless devices. WPA2 differs from WPA in that it includes the **AES** (**Advanced Encryption Standard**), a strong cryptographic technology required by the U.S. government and some corporations. For authentication, WPA2 uses the same methods as WPA.

How to choose. To protect network transmissions and sensitive information, your wireless network should operate with the strongest encryption method supported by your wireless AP and devices. Of the three options for securing wireless transmissions, WPA2 is the newest and most secure technology.

Some wireless APs can accommodate a mixture of wireless technologies, and others require you to select only one. For example, if your wireless AP supports WPA2 mixed mode, it can handle WPA and WPA2 on the same SSID. An alternative, if the wireless AP supports it, is to create multiple SSIDs, each with a different wireless security standard.

If your wireless AP limits the network to a single security standard, all of your devices must support it. To use WPA2, for example, the wireless AP and your wireless devices (notebooks, PDAs, barcode scanners) must also support WPA2. (The Wi-Fi Alliance maintains a list of WPA and WPA2 certified devices at certifications.wi-fi.org/wbcs_certified_products.php.) The following information discusses each technology in more detail.

WEP. WEP is considered unsecure, primarily because the encryption key is static and does not change. However, if WEP is your only alternative, it is more secure than no encryption at all. And unlike WPA and WPA2, WEP operates on Win98/Me/XP systems. WPA and WPA2 work with WinXP only.

To use WEP, first configure your wireless AP (as we mentioned earlier, you'll use your browser and admin software). If possible, select 128-bit encryption, which is stronger than 64-bit encryption. For the passphrase, use a combination of hard-to-guess letters and numbers appropriate for a strong password. After saving this information on the wireless AP, configure the same settings on your wireless devices and test device connectivity.

WPA. WPA was an interim solution to WEP security issues, and it implements many of the security improvements of WPA2. If your wireless devices currently support only WEP, you may be able to upgrade them to WPA. Check the device vendor's Web site to determine whether there is an update available.

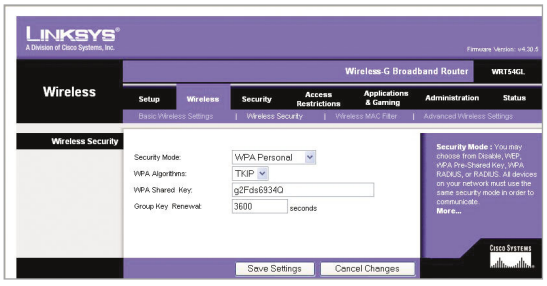
For encryption, WPA uses the TKIP (Temporal Key Integrity Protocol). Rather than relying on a single, fixed key, TKIP makes the encryption key more difficult to guess because it changes regularly. In addition, the WPA encryption process uses multiple keys derived from a master key, rather than simply a single master key as with WEP.

To use WPA, your network needs:

- A wireless access point that supports WPA
- Client devices with an OS and a network adapter that support WPA

Computers running WinXP SP2 support WPA. You also need a wireless network adapter and driver enabled with WPA in order to select WPA encryption and authentication options in the wireless network properties. Finally, your wireless AP must also be configured for WPA.

WPA offers two options for authentication. For personal and SOHO use, WPA comes with a PSK (preshared key) option. This is a simple method of authentication to implement because it only requires you to enter a secret set of characters on the wireless AP and each device that accesses the network. To activate WPA-PSK, select it on your wireless AP and enter a set of characters for the shared key, choosing characters similar to a strong password. Enter the same information in your device's wireless connection configuration and test connectivity.



To encrypt your wireless network transmissions, set your wireless access point to use the most advanced encryption method that your wireless devices support.

For corporations, WPA provides the 802.11x port-based network access control with EAP (Extensible Authentication Protocol) authentication method. It supports stronger security than PSK because it requires an authentication server, such as a RADIUS (Remote Authentication Dial In User Service) server, to control access to the network. However, small businesses or employees working from home can use WPA-EAP with additional software.

WPA2. Similar to WPA, WPA2 uses the PSK and 802.1x with EAP methods for authentication. However, the encryption standard for WPA2 is AES, whereas WPA uses TKIP. AES provides strong encryption, and it is the standard adopted by the U.S. government to protect sensitive data.

To use WPA2, your network needs:

- A wireless access point that supports WPA2
- Client devices with an OS and a network adapter that support WPA2

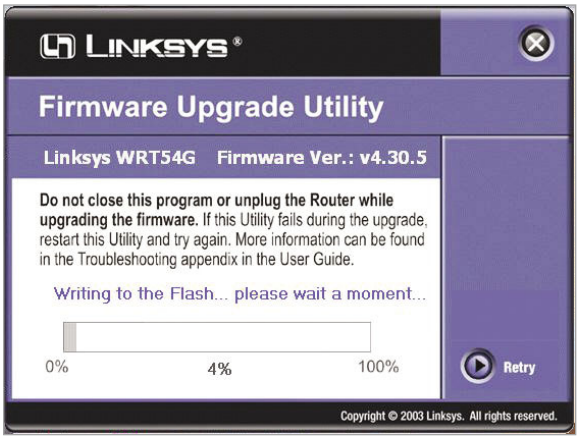
If you already own a wireless AP, you can check with the manufacturer to determine whether it's upgradeable to WPA2. Wireless APs released in 2003 or after that support 802.11g devices probably support WPA2 with a firmware update. If your wireless AP does not support WPA2, you can use WPA or WEP.

Whether you can use WPA2 also depends on whether your wireless devices' operating systems support it. Similar to the wireless access point, some wireless network adapters are upgradeable to WPA2 with a firmware update from the manufacturer. You must also update the adapter driver.

WinXP is the only Windows OS with WPA2 capabilities. Windows-based wireless notebooks must run WinXP with SP2. In addition, Microsoft released a WPA2 update for WinXP SP2 that you must install. For details about the WPA2 update, see the Microsoft Help And Support article at support.microsoft.com/?id=893357.

After you install the WPA2 update, WinXP's Choose A Wireless Network dialog box designates any WPA2-enabled networks with "security-enabled wireless network (WPA2)." The wireless connection Properties dialog box adds WPA2 (corporate/enterprise networks) and WPA2-PSK (personal networks) options to the Network Authentication drop-down box on the Association tab. Note that the WPA2 options are available only if your wireless network adapter and its driver support WPA2.

To activate WPA2 on your SOHO wireless network, select WPA2-PSK on the wireless AP and type a set of characters for the shared key, choosing characters as you would a strong password. Enter the same information in your device's wireless connection configuration and test connectivity.


LINKSYS®
Firmware Upgrade Utility
Linksys WRT54G Firmware Ver.: v4.30.5
Do not close this program or unplug the Router while upgrading the firmware. If this Utility fails during the upgrade, restart this Utility and try again. More information can be found in the Troubleshooting appendix in the User Guide.
Writing to the Flash... please wait a moment...
0%
4%
100%
Retry
Copyright © 2003 Linksys. All rights reserved.

You can add the newer encryption technologies (WPA and WPA2) to an existing wireless AP through a firmware update from the manufacturer.

Layers Of Security

Securing a wireless network requires layers of defense. Multiple layers of defense for wireless networks include changing the administration tool password, modifying the SSID default settings, filtering devices by MAC address, and employing the highest encryption/authentication security possible. Implementing the strategies discussed here will make it difficult for others to detect or access your wireless network. RS

BY CARMEN CARMACK

Summing It Up

To help you differentiate between wireless authentication and encryption technologies, the table below provides a summary of the differences among the three main methods.

	WEP	WPA	WPA2
Authentication	Open (none) or manually configured shared key	SOHO/Personal: manually configured PSK (preshared key) **Enterprise:** 802.1x EAP with RADIUS server	SOHO/Personal: manually configured PSK (preshared key) **Enterprise:** 802.1x EAP with RADIUS server
Encryption	WEP-RC4 cipher	TKIP-RC4 cipher	CCMP-AES cipher
Key Type	Static	Dynamic	Dynamic
Key Length	40 or 104 bits	128 bits	128 bits
Key Derivation	Single master key	Multiple keys derived from a 256-bit PMK (pairwise master key)	Multiple keys derived from a 256-bit PMK (pairwise master key)
Windows OS Support	Windows 98/Me/XP	Windows XP SP2	Windows XP SP2 with WPA2 Update

Troubleshooting Essentials

Fixes For 19 Common Home Networking Problems

Home networking is easily one of the most brilliant inventions of the computer age. No longer isolated islands unto themselves, each PC on your network can share files and access the Internet just like a computer at an office. And, thankfully, the process of building a home network is typically just a matter of buying a router and running Ethernet cable to each computer, then enabling a few simple Windows settings or clicking a few icons. For anyone who has installed a home network, the benefits become quickly apparent: less time copying files to a floppy disk, external hard disk, or flash drive; more Web browsing from every PC; and even some unique advantages such as sharing a printer or performing network backups.

Of course, with any major upgrade to your home computer system, there are challenges. Some troubleshooting problems are quite simple—just click one checkbox to enable an icon in the Taskbar. Other fixes require that you dig around in control panels and system settings. Yet, most conflicts are easier to resolve than you might think, mostly because there is typically just one setting to tweak. Often, there's just one Windows XP option enabled by mistake. Network data either flows freely (and without problems) or usually has one simple roadblock. The good news is that, once you fix the roadblock, it's easy to see when the network is running smoothly again.

Q I don't see an icon on my Windows XP taskbar for accessing my network settings. Where did it go?

A Here's one of the most common, yet frustrating, problems that can occur in WinXP. The reason it's common is that the icon you can use to access network settings is not enabled by default. So, if you normally see the icon—which looks like two small computers next to each other—at work, and then on a home network you can't see the icon, you might wonder if something is wrong. It's also frustrating because it's difficult to figure out how to enable the icon for easy access. To find the option, go to Start, then Connect To, then Show All Connections. All the icons for your network connections will appear, including any wired or wireless connections. Right-click the Local Area Connection icon and select Properties. Now, place a check in the Show Icon In Notification Area checkbox and click OK. The icon will now appear.

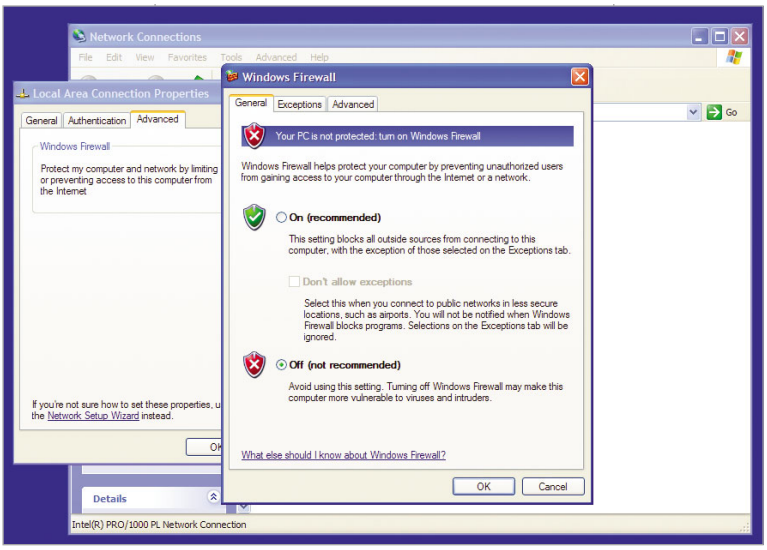
Q When I access My Network Places, why can't I see any other networked computers?

A In a vast majority of cases, not seeing any other computers when you go to My Network Places has more to do with physical connections than actual Windows settings or drivers. So, the first troubleshooting tip is always to make sure your Ethernet cables are plugged in securely to your PCs and into the router. The next step is to make sure the PCs are all turned on and that you have enabled file sharing. To enable file sharing, click Start, click My Computer, right-click the appropriate drive icon under Hard Disk Drives, select Sharing And Security, agree to the warning (if any) by clicking the link, and click to select the Share This Folder On The Network checkbox; if the Enable File Sharing dialog box appears, click the Just Enable File Sharing radio button and click OK. A third step is to make sure the router is powered on. One last common resolution is to remove any Network Bridge that is shown in Network Connections. Go to Start, Connect To, and Show All Connections. Right-click the Network Bridge and select Delete. (Windows XP sometimes tries to bridge FireWire and Ethernet networks by mistake.)

Q When I access My Network Places I see a few computers, but why don't I see the one that has the files I need to transfer?

A It's important to check the obvious causes first: make sure the PC you want to access is powered on, double-check the Ethernet connections to both the computer and the router to make sure they are secure, and to enable file sharing on the PC in question. To enable file sharing, click Start, click My Computer, right-click the appropriate drive icon, select Sharing And Security, agree to the warning (if any) by clicking the link,

and click to enable the Share This Folder On The Network checkbox. If the Enable File Sharing dialog box appears, click the Just Enable File Sharing radio button and click OK.


Network Connections
Local Area Connection Properties
Windows Firewall
General
Exceptions
Advanced
Your PC is not protected: turn on Windows Firewall
Windows Firewall helps protect your computer by preventing unauthorized users from gaining access to your computer through the Internet or a network.
On (recommended)
This setting blocks all outside sources from connecting to this computer, with the exception of those selected on the Exceptions tab.
Don't allow exceptions
Select this when you connect to public networks in less secure locations, such as airports. You will not be notified when Windows Firewall blocks programs. Selections on the Exceptions tab will be ignored.
Off (not recommended)
Avoid using this setting. Turning off Windows Firewall may make this computer more vulnerable to viruses and intruders.
What else should I know about Windows Firewall?
OK
Cancel
Details
Intel(R) PRO/1000 PL Network Connection

Conflicts can occur on a network if you run more than one firewall. You can disable the Windows XP firewall if you already use, say, Norton Personal Firewall.

Q When transferring files from another computer, why does the transfer take much longer than I expect?

A Slow file transfers is one of the more frustrating problems that occurs on a home network. One day your files transfer quickly, and the next day they seem to move across the network like molasses. Yet, the most probable cause for this issue is almost always due to network congestion. This traffic can occur for many reasons, however. Someone else in your home may be downloading large files from the Internet or from another PC. Another probable cause is due to spyware or a virus that is consuming network resources. Run a free virus checker such as Trend Micro's Housecall (housecall.trendmicro.com) and perform a spyware scan using a program such as Spybot Search and Destroy (www.safer-networking.org) to remove any network-hogging applications.

Q When transferring files from another computer, why does the transfer sometimes end suddenly?

A The most common reason for an abrupt file transfer termination is due to the other computer either entering hibernation mode (if the other computer is a laptop) or powering down the hard drive to save energy, which can occur on a desktop or laptop. WinXP typically does not disable these power-saving functions on the **client computer** (the computer from which you are transferring data). You can avoid this problem by disabling power savings functions. Go to Start, click Control Panel, and then double-click Power Options. Select Never in all of the drop-down menus on the Power Schemes tab. Another common cause of sudden file transfer termination, especially when working with very large files, has to do with data corruption. Make sure you run disk defragmentation on all network computers. Go to Start, click All Programs, click Accessories, click System Tools, select Disk Defragmenter, and start the disk cleaning and defragmentation.

Q When I access My Network Places in Windows XP, my computer starts searching for other computers on the network but the hourglass never goes away. I have to reboot. Why does this happen?

A If WinXP is not able to access any of your computers, and shows the hourglass for a long period trying to find other computers on the network, you may have an IP (Internet Protocol) address conflict on the network. An IP address is like a mailing address: it must be unique. Your home router assigns an address (for example, 192.168.2.10) to each computer. The easiest solution is just to power down the router and all computers, and then to turn on the router and then the computers one-by-one. If you are using two home routers, IP conflicts are much more common. To solve duplicate IP addresses with multiple routers, you will need to change the router's IP address range. Contact the router manufacturer's technical support for the steps to perform that action.

Q Why does a pop-up message appear saying that my computer has "little or no connectivity"?

A This balloon pop-up message, which appears in the lower-right corner of your computer display, can appear momentarily when your PC first attaches to the network. What's happening is that your home router is assigning an IP address to your PC, and during this process, you won't be able to access the Internet or other computers. In a few seconds, your PC will likely connect just fine. If you see the message, but still can't access other computers, it's because the router is not handing out IP addresses correctly due to a network conflict. The fix is usually to just power down the router, and turn it on after about 30 seconds, to clear out any conflicts. Otherwise, it could also be a setting on the router, in which case you should consult the router documentation or call tech support and explain the error message you are seeing.

Q Why doesn't the one particular folder I need to access through my network appear after I connect to another networked computer?

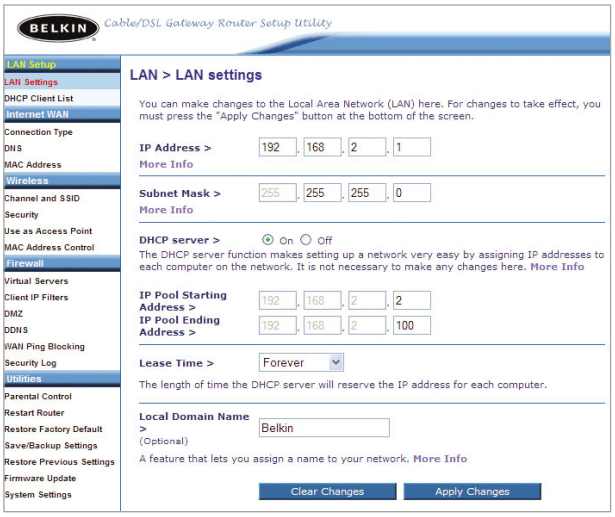
A If you can see the network shares from all of your computers on a home network, but not one particular folder, then the solution is to enable file sharing for that specific folder. To enable file sharing click Start, click My Computer, right-click the hard drive icon representing the computer that is not sharing the folder, select Sharing and Security, agree to the warnings (if any) by clicking the link, and click to check the Share This Folder On The Network checkbox. If the Enable File Sharing dialog box appears, click the Just Enable File-Sharing radio button and click OK.

Q Why can I access the files on another computer on my network but not edit any of the documents? The documents open as "read only" in an application such as Microsoft Office.

A Seeing a "read only" message when you open a document you are accessing across a network is almost always caused by this issue: The document is already open on one of the networked PCs. WinXP attempts to protect documents from damage by making them read-only when they are open on another computer. The solution is just to close the document on the other computer. However, occasionally a document, such as a word processing file, will become "stuck" in a state of this network protection, even though it is closed. The solution is to go ahead and open the file as read-only, and then just save the file using a new name. You can then delete the original file and rename the newly saved document to match the original document.

Q I ran the Network Setup Wizard but I still can't connect to other computers on my network. Why don't they appear in My Network Places?

A The Network Setup Wizard, which runs when you enable file sharing for a hard drive on your computer, is sometimes a cause for network problems rather than a way to make networking run smoother. One issue is that the wizard can create a "network bridge" between connection types—such as FireWire and Ethernet—when you don't want one. Or WinXP may enable the WinXP firewall, causing a conflict if you already run a firewall such as Norton Personal Firewall on your computer, or a different firewall that runs on your router. To delete a network bridge, go to Start, click Connect To, and click Show All Connections. Right-click the Network Bridge and select Delete. To disable the WinXP firewall, right-click your network icon on the Taskbar, select Change Windows Firewall Settings, select Off, and click OK. Also, make sure you check the physical Ethernet connections to see if they are plugged in securely and reboot the router.


BELKIN
Cable/DSL Gateway Router Setup Utility
LAN Setup
LAN Settings
DHCP Client List
Internet WAN
Connection Type
DNS
MAC Address
Wireless
Channel and SSID
Security
Use as Access Point
MAC Address Control
Firewall
Virtual Servers
Client IP Filters
DMZ
DDNS
WAN Ping Blocking
Security Log
Utilities
Parental Control
Restart Router
Restore Factory Default
Save/Backup Settings
Restore Previous Settings
Firmware Update
System Settings
LAN > LAN settings
You can make changes to the Local Area Network (LAN) here. For changes to take effect, you must press the "Apply Changes" button at the bottom of the screen.
IP Address > 192 . 168 . 2 . 1
More Info
Subnet Mask > 255 . 255 . 255 . 0
More Info
DHCP server > On Off
The DHCP server function makes setting up a network very easy by assigning IP addresses to each computer on the network. It is not necessary to make any changes here. More Info
IP Pool Starting Address > 192 . 168 . 2 . 2
IP Pool Ending Address > 192 . 168 . 2 . 100
Lease Time > Forever
The length of time the DHCP server will reserve the IP address for each computer.
Local Domain Name > Belkin
(Optional)
A feature that lets you assign a name to your network. More Info
Clear Changes
Apply Changes

If you happen to use two routers in your home, you may need to set the IP (Internet Protocol) range for one router so that it does not conflict with the other router.

Q Why do I keep seeing a folder shared from another computer on my network even though that computer is turned off?

A Here's a networking issue that seems to confound many users, even though it is entirely innocuous. These "ghosted" file shares appear because WinXP will still show network folders for up to 48 hours after they were last available. If you double-click the icon, you won't see the network files if the PC is off or file sharing is disabled for that folder. The only solution is to reboot, or just wait another day or two, and the ghosted file shares will not appear.

Q I just installed a new network drive. Why can't I see it on my home network?

A A NAS (network-attached storage) drive, such as Maxtor's Shared Storage Plus, is handy because you can store all your important files on the drive. The drive is not connected to a PC directly and is available at all times, makes network backups, and even accesses the files remotely from an Internet connection across town. The main reason a network drive might not be available from a PC on your network is due to a configuration problem with the drive itself. You should check the physical connections just to make sure there are no loose wires, but typically it just means running the setup program on the CD that came with the drive, and making sure the drive is configured properly for your router and the network. If you change how the network drive is plugged into your router, or installed a new router, you will need to run the setup program.

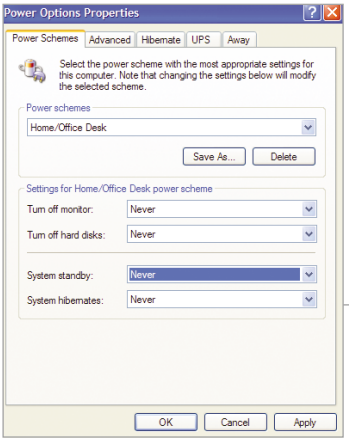
Q Why do I receive a "File or network path no longer exists" error message when I try to open another file on a networked computer?

A This error can appear when you try to access a file or folder using a shortcut that is no longer valid. In the old days, Windows required a

network map to a remote drive, but now WinXP manages all folder and file sharing on its own. A shortcut is just a faster way to access one particular folder, but Windows does not correct the shortcut if you move or delete the remote folder. The solution is just to browse My Network Places (click Start, then My Network Places) and double-click the computer to access and files or folders. You can also manually correct network folder shortcuts.

Q Why might I receive an error message that says a computer "is not accessible" and that I "might not have permission to use this resource…"?

A This error can occur when the file sharing on the remote computer is configured for guest access only or when only certain folders are available for editing. You might open one folder that is unprotected and then try to access a subfolder that holds private files. The solution is to enable more access on the client (remote) computer. Right-click the folder you want to access, and click the Sharing tab. Make sure the Allow Network Users To Change My Files checkbox is checked. Also, uncheck the Make This Folder Private Checkbox and click OK. RS



Power settings on a desktop or laptop computer can sometimes interfere with networking. To make sure a PC is available at all times disable the settings for turning off a hard drive.

BY JOHN BRANDON

Troubleshoot Internet Access Through A Home Network

Q None of my networked computers can access the Internet over my network. Even when I connect my cable or DSL (Digital Subscriber Line) modem directly to one PC, the Internet is still not working. Why?

A The most common cause for this problem is that the modem is not properly provisioned. You may need to call your Internet service provider and ask them to provision your modem for Internet access. They will essentially add your modem to the Internet. Check the modem by connecting it to your computer using an Ethernet cable before trying to connect the modem to a router and sharing the connection with all your PCs.

Q All of my computers can access the Internet over my home network except one. Why?

A There are two probable causes. There might be a problem with the physical connection between PC and router. Check to make sure the cable is securely connected. Another cause is due to an IP (Internet Protocol) address conflict, which can often occur if you are using two routers or happened to power-on two computers at about the same time. The solution is typically just to reboot the router and the PCs.

Q Why, when I access the Internet over my home network, do Internet downloads go slowly, even though I have a fast connection?

A One cause for Internet file transfer slowdowns, similar to what happens when you are copying files between computers on the network, is congestion. If too many people in your home are trying to download large files or watch streaming video files (movies that play directly from a Web site), then all users on the network will experience traffic slowdowns. The best tip is just to use one PC for most of your large file downloads or video streaming. Another idea is to increase the broadband speed on your cable or DSL modem. Just call your provider and inquire about faster speeds (such as 5Mbps [megabits per second]) and the related pricing plans.

Q Why can I share files across my network, but not access the Internet?

A This problem occurs when your cable or DSL modem is not connected or provisioned for the Internet. The router is functioning fine, but it is not able to share the Internet connection. Most routers have several indicator lights. For example, an Internet light will shine steady when the Internet is available for network access. Check the physical connections first, then call your cable or DSL provider to ask about provisioning or troubleshooting the connection. (Typically, they can tell you if the modem should be functioning properly by running a simple test.)

Q I connected my video game console to a home network. Why can't it access the Internet for multiplayer games?

A One of the most common reasons why a Microsoft Xbox 360 or Sony PlayStation 2 cannot access the Internet is due to how these devices try to establish an Internet connection. They are usually preconfigured to use a static IP address, not a dynamic IP address. If you connect the console to your router, you'll need to enable infrastructure mode. On an Xbox or Xbox 360, for example, there is a step in the sign up process that prompts you to choose whether to assign a dynamic IP address. Enable that option so the router assigns the address. I

Communication Breakdown

General Troubleshooting Tips

Networks are the main reason that nearly every business has an IT department—and for good reason. Networks are tricky to set up and even more difficult to secure. They stall out or work in fits and start for seemingly no reason. It's all worth the effort, though, when you're able to stream multimedia files to a multitude of devices throughout your home, share files easily among computers, and give all of your computers access to the same broadband Internet connection. Whether you're setting up a home network for the first time or are trying to troubleshoot problems with your existing network, this guide, along with a willingness to tweak some settings, should get everything on track.

Hardware & Configuration Issues

Problem: I have two computers located near one another; I connected them using a single Ethernet cable, but they are not networked.
Solution: It's tempting to try to network a couple of computers by linking them with a cable, but this isn't the most efficient method. If you opt to go this route, you'll need a special kind of Ethernet cable called a crossover cable such as the 7-foot-long Geek Squad Cat-6 Crossover Cable (22.99; www.bestbuy.com). You'll also need to assign static IP (Internet Protocol) addresses to each computer, which we'll discuss later in the article. In addition, you'll need to install two NICs (network interface cards; available for as little as $10 and up to $199) in at least one of the computers on the network in order to share a broadband Internet connection. Instead of a crossover cable connection, we recommend investing in a router, such as the Linksys WRT54GS ($79.99; www.linksys.com). With a router, you can connect multiple computers on your network and easily share an Internet connection among all of them.

Problem: I bought a hub with several ports to share a broadband Internet connection among multiple computers, but it doesn't seem to work.
Solution: When you have a hub or switch, you can't simply plug your computers into some Ethernet ports and then plug the Ethernet cable from your broadband modem into a remaining port and expect it to work. For that job you'll need a router (sometimes called a gateway or access point), which has the built-in hardware that is necessary to manage the incoming broadband connection. (Every router comes with a built-in switch, and they're all compatible with additional switches via the uplink port.) See the online-only sidebar titled "Putting It All Together: Network Hardware In Action" (www.smartcomputing.com/extra/networking) for more details on the differences between routers, hubs, switches, and other networking devices.

Problem: My network cable doesn't fit into any of the ports on the back of my computer or the cable is too small for the ports on the back of the router.
Solution: Newcomers to networking commonly confuse the Ethernet port on their NIC and the phone jack on their dial-up modem. The two ports have the same basic shape, but phone jacks are much smaller than Ethernet ports, so if the Ethernet cable from your router doesn't seem to fit in your computer's port, you're most likely trying to connect the cable to the wrong port. Most computers today have a built-in Ethernet port, but if yours doesn't you'll need to install a NIC or use a USB Ethernet connection.

Problem: One of my router ports doesn't seem to work, no matter what device I plug into it using an Ethernet cable, even though those devices work fine when connected to the other ports.
Solution: You may be plugging the device into the router's uplink port, which usually has the label Uplink printed above or beneath it. These ports are not meant for devices. Instead, you can use them to add another hub or router to your existing router, which then makes more ports available for other devices. If you have a wireless router and want to connect more devices than the router has ports, connect everything you can wirelessly. Most wireless routers can support dozens of wireless devices simultaneously, ridding you of the need to buy extra hardware (not to mention running a bunch of cable). (See

the article titled "Wireless Woes" on page 138 for information on troubleshooting wireless networks.)

Alternatively, you may have plugged a computer or another device into the WAN (wide-area network) port, which is reserved for the Ethernet cable coming from your broadband Internet connection's modem. Don't ever plug anything into the WAN port other than the broadband modem.

Problem: My cable or DSL (Digital Subscriber Line) modem came with both USB and Ethernet ports, and I plugged them both into the computer, but I can't get on the Internet from that computer or any other computer on the network.

Solution: This is a common problem with modems from broadband Internet access providers, and the golden rule is to connect one cable or the other but never both. If the computer has an Ethernet port we recommend using that. Better still, instead of connecting the modem directly to a particular PC, use an Ethernet cable to connect it to the WAN port of a router (wireless or otherwise). This lets any computer or networked device on the network access the Internet connection without requiring that any particular computer be turned on before the connection is available.

Problem: I need to configure my router, but there doesn't seem to be any software available that lets me access the settings.

Solution: Contemporary routers all operate from a Web-based interface, so there are no drivers or applications to install to get at their settings. Just open your favorite Web browser and type the router's IP address (which is listed in the user manual) in the browser's Address bar, just as you would enter the URL of a Web site you want to visit. For example, D-Link routers have the default IP address 192.168.0.1, so typing that string of digits in the browser opens the router's configuration page.

Problem: I typed the correct IP address to configure my router but now it's asking me for a username and/or password even though I haven't established one yet.

Solution: Securing your router with a password is very important, but when the router is first installed it may ask for a password (and sometimes a username) before you can get into the options screen to set your own password. Sometimes, you can leave these fields blank, but most often you can type **admin** as the default username and password. If this doesn't work, experiment with variations: Leave the username blank and type **admin** as your password and vice-versa. The default password is also listed in the router's user manual. Be sure to change the default password as soon as possible, as it is your first line of defense against network hackers.

Problem: I established a password for my router but forgot it, and now I can't get in to adjust settings or update the firmware.

Solution: Router passwords are designed to keep intruders on the Internet from cracking into your network, but they are very easy to bypass for people—like you—who have physical access to the router. Most routers have a reset button embedded somewhere in the back of the device that reverts the router to its factory-default settings. If you forget your password, just hold down the reset button for 10 seconds or so, release it, and the router should work with the default password listed in the user manual. If that doesn't work check the manual to see if the router uses a different reset routine; for instance, sometimes you must disconnect the power or perform certain steps in order to return the device to its default state.

Problem: I use a wireless network and have configured WEP [or another security system] on all of my wireless devices, but I can't figure out where to configure those settings on computers that I've physically connected to the network using cables.

Solution: WEP (Wired Equivalent Privacy) and other wireless security standards apply only to wireless devices, so you don't need to worry about them when configuring computers or other devices tethered to the network with Ethernet cables.

Instead of using a crossover cable, get a router such as the Linksys WRT54GS ($79.99; www.linksys.com) to connect your computers and other network devices.

Problem: My router doesn't have enough Ethernet ports to accommodate all of my network devices.
Solution: You can buy an inexpensive switch (make sure it's a switch, such as the Linksys SD208 8-port 10/100/1000 Gigabit Switch [$71.99 at Newegg.com] and not just a hub) that has additional ports and connect it to the uplink port on the back of the existing router; however, we'd recommend that you go wireless instead. A wireless router may only have four or five Ethernet ports on the back available for wired network connections, but it supports dozens of wireless network devices simultaneously.

Problem: I want to be able to back up files to a central location from anywhere on the network; however, I always have to turn on the computer with the backup drive installed before I do this.
Solution: Each computer on the network has a hard drive installed, and you can store data on any of those drives from any other computer attached to the network. However, there's a catch: The computer housing the drive to which you want to save the backup must be turned on before it's accessible to the rest of the network. As a workaround, we suggest you invest in a NAS (network-attached storage) device, such as the Plextor PX-EH25L 250GB NAS device ($299; www.plextor.com). These devices operate independently of any computer on the network, and they contain at least one hard drive and all of the hardware you'll need to connect them to the network. Connect the NAS device to the network using an Ethernet cable (or wirelessly, if the device supports that type of connection) and leave it on all of the time.

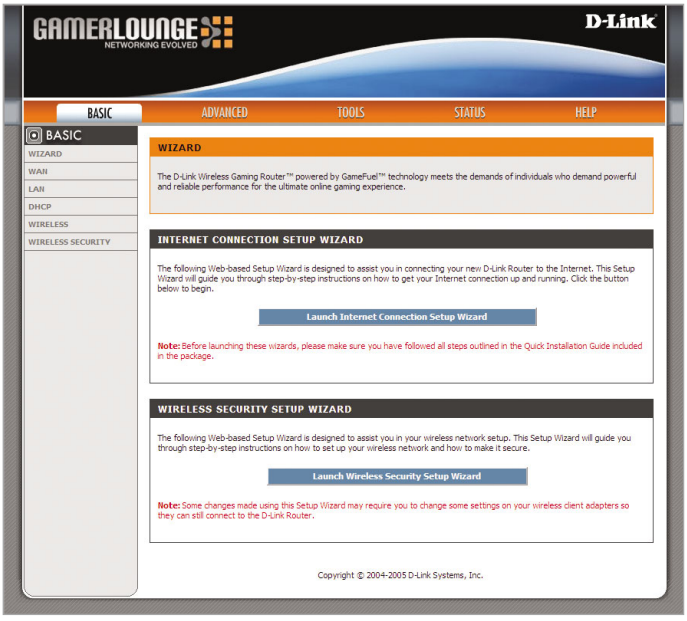
Problem: I have a network printer, but after I installed it, I have to turn on one specific computer on my network before other computers on the network can access the printer.
Solution: Make sure you've attached the printer directly to the router using an Ethernet cable and not to a particular PC via a USB or another connection. Then, install the printer as a network printer and not as a local printer. To do this in Windows XP click Start, click Control Panel, and double-click Printers And Other Hardware (or Printers And Faxes if you are in Classic View). Click Add A Printer, click Next, select the A Network Printer, Or A Printer Attached To Another Computer radio button, and click Next. Select the Browse For A Printer radio button, click Next, and click the entry for the printer. Then, click Next, select Yes if you want to use that printer as the Default printer, and click Next to complete the installation. Keep the printer drivers handy because Windows may ask for them during the installation process.

Problem: Sometimes, my ISP (Internet service provider) or a program I'm using demands that computers on my network use a static IP address, but I have no idea what that means or how to assign one to each PC.
Solution: Each device on the network has an IP address, and if you use a router, it assigns an IP address to each connected device on its own. When you turn off a networked device, the IP address it had is freed, and the router can then assign it to any other device that shows up on the network. IP addresses assigned this way are called **dynamic IP addresses** because they constantly shift, but you can use your router and Windows to assign each computer a **static IP address** that never changes.

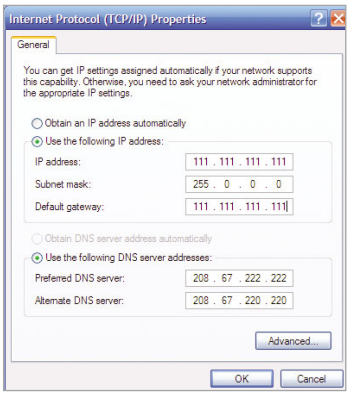
Modern routers assign IP addresses using DHCP (Dynamic Host Configuration Protocol), so you'll need to look at the manual that came with your router to find out how to access the DHCP settings and then add your computers to the router's static DHCP client list. You'll also need to know the MAC (media access control) address for each computer's NIC (most modern routers should be able to take care of this info for you), and you should write down the IP address the router assigns to each computer because you'll need that information for the next step.

You also need two other pieces of information: the router's Subnet Mask and Default Gateway. To locate that info in WinXP, click Start and click Run. Then, type **cmd** and press ENTER. Type **ipconfig /all** at the prompt and write down the numbers you see next to the Subnet Mask and Default Gateway entries.

Now you need to let each PC know what its new permanent address is. In WinXP click Start, My Network Places, and View Network Connections; right-click Local Area Connection (or the entry that matches the PC's


GAMERLOUNGE
NETWORKING EVOLVED
D-Link
BASIC
ADVANCED
TOOLS
STATUS
HELP
BASIC
WIZARD
WAN
LAN
DHCP
WIRELESS
WIRELESS SECURITY
WIZARD
The D-Link Wireless Gaming Router™ powered by GameFuel™ technology meets the demands of individuals who demand powerful and reliable performance for the ultimate online gaming experience.
INTERNET CONNECTION SETUP WIZARD
The following Web-based Setup Wizard is designed to assist you in connecting your new D-Link Router to the Internet. This Setup Wizard will guide you through step-by-step instructions on how to get your Internet connection up and running. Click the button below to begin.
Launch Internet Connection Setup Wizard
Note: Before launching these wizards, please make sure you have followed all steps outlined in the Quick Installation Guide included in the package.
WIRELESS SECURITY SETUP WIZARD
The following Web-based Setup Wizard is designed to assist you in your wireless network setup. This Setup Wizard will guide you through step-by-step instructions on how to set up your wireless network and how to make it secure.
Launch Wireless Security Setup Wizard
Note: Some changes made using this Setup Wizard may require you to change some settings on your wireless client adapters so they can still connect to the D-Link Router.
Copyright © 2004-2005 D-Link Systems, Inc.
Most routers are configured directly from a Web browser.

NIC) and click Properties. Click Internet Protocol (TCP/IP) to highlight it and click Properties. In the General tab, select the Use The Following IP Address radio button and type the IP address that your router assigned to that particular computer. Then, type the Subnet Mask and Default Gateway numbers you wrote down and click OK. Repeat this process for each computer on the network, keeping in mind that the IP address numbers should always be different, but the Subnet Mask and Default Gateway entries should be the same for all of the computers on your network. Reboot each computer when you've finished entering the information, and the program that requires a static IP address should work.


Internet Protocol (TCP/IP) Properties
General
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
111 . 111 . 111 . 111
Subnet mask:
255 . 0 . 0 . 0
Default gateway:
111 . 111 . 111 . 111
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
208 . 67 . 222 . 222
Alternate DNS server:
208 . 67 . 220 . 220
Advanced...
OK
Cancel

Static IP addresses, subnet masks, and gateways must be entered manually into WinXP's Internet Protocol (TCP/IP) Properties page.

File & Internet Sharing Problems

Problem: I want to share files among my networked computers, but Windows won't let me.

Solution: For security reasons file sharing is not turned on by default just because the computers are networked. You need to enable file sharing manually either for certain folders, the entire drive, or just for certain files if you want to restrict access.

In WinXP, to enable file sharing for the entire drive, click Start and My Computer, right-click the icon for the drive you want to share, and click Properties. Select the Sharing tab, click the warning if you have WinXP Home Edition to get rid of it, and then if necessary click the If You Understand The Security Risks But Want To Share Files Without Running The Wizard, Click Here link. Select the Just Enable File Sharing radio button and click OK.

If you performed the previous steps or already had access to entries in the Network Sharing And Security box put a check mark in the Share This Folder On The Network box. Give the drive a name (the drive letter generally works best). If you want other people on the network to be able to modify and delete files on the shared drive, put a check in the Allow Network Users To Change My Files box. Click Apply and you'll see a hand under the drive's icon to indicate that it is now shared. You can share individual folders if you don't want to share the entire drive by right-clicking the folder, clicking Properties, selecting the Sharing tab, and putting checks in the boxes as described for drive sharing.

This method also works for CD and DVD drives, so you'll be able to use the DVD drive on one computer to install software to another computer on the network. Right-click the icon for the CD or DVD drive and follow the steps outlined for sharing the hard drive.

Problem: Even when I've enabled file sharing, WinXP won't let me see certain folders I try to access from other computers on the network.

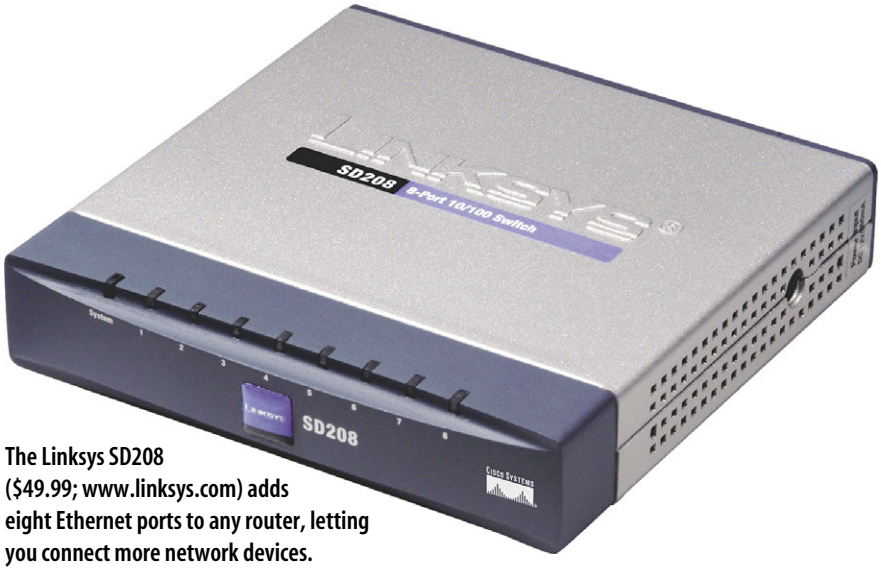
Solution: WinXP has more robust security features than previous versions of the operating system, and one setting prevents users on one PC from accessing files stored in particular folders on another networked PC. For example, if you want to access something on one computer's Desktop from another computer on the network, WinXP won't let you because Desktop files are stored in the Systems folder, which is off-limits even if you've shared the entire hard drive. Be sure to put everything you want to have network access to in the Shared Documents folder or in a folder that isn't on the Desktop or in another protected folder (like the Systems folder).

Problem: When I use a WinXP computer to access other computers on the same network it takes a long time (sometimes several minutes) to even see them.

Solution: This is a known problem with the way WinXP handles the shortcuts in the Network Neighborhood menu. Because of a programming glitch, the shortcuts generate network traffic to the point where they can completely saturate the connection and bring the network to a halt for anywhere from several seconds to several minutes. Sometimes things degenerate to the point that the main program behind WinXP (Explorer.exe) crashes, bringing the Desktop or sometimes the entire computer down with it. If you have WinXP and are experiencing these problems when attempting to access other computers on the network, then use Windows Update to download all of the latest patches and hotfixes for WinXP and see if that solves the problem. Click Start, expand All Programs, and click Windows Update. Click Custom, wait for the scan to complete, click Review And Install Updates, and put checkmarks in all entries in the High Priority section before clicking Install Updates. Reboot the computer and see if you can now browse the network without trouble.

If not, you need to visit the Microsoft Support site (support.microsoft.com/contactus/?ws=support) and/or contact Microsoft customer support by phone or email. Explain that you need the hotfix file referenced in the Microsoft Knowledge Base article 841978: The Explorer.exe Process Stops Responding When You Use Network Shortcuts In Windows XP.

Problem: I can't see other computers that are on my network.



The Linksys SD208 ($49.99; www.linksys.com) adds eight Ethernet ports to any router, letting you connect more network devices.

Solution: Double-check the workgroup name for each computer to make sure they are all the same and try restarting all of the computers to see if that forces them to make their presence known. This also sometimes happens when an early version of WinXP is trying to see computers that have earlier versions of Windows installed across the network, but updating WinXP using the procedure detailed in the previous tip should fix the problem.

Problem: My computers are on a network, but only one of them has Internet access.

Solution: Sharing Internet access is one of the key reasons to set up a home network, but it may be confusing because there are two way to go about it. The easiest way is to use a router and attach the broadband Internet modem to the router's WAN port using an Ethernet cable. If the cable from the modem is connected directly to a PC, this method won't work, and you'll need to either switch over to the router method or enable Internet Connection Sharing.

If the computer with the Internet connection you want to share uses WinXP, click Start, My Network Places, and then Set Up A Home Or Small Office Network. When the Network Setup Wizard appears, click Next, click Next again, and select the This Computer Connects Directly To The Internet Radio button. Click Next, click the icon that corresponds to the NIC where the Internet connection comes in (this usually is labeled Local Area Connection), and click Next. Give the computer a description and a name, click Next, type a workgroup name (use the same one for all computers), and click Next. Choose the radio button that corresponds to the file and printer sharing settings you want to use, click Next, and click Next again to complete the setup.

You'll need another NIC installed in the computer with the Internet connection, so it has an outgoing connection to the rest of the network. (You can connect the second NIC to a hub or switch using a standard Ethernet cable or directly to the NIC of another computer using an Ethernet crossover cable.) Once everything is connected, boot up the other PCs on the network and repeat the setup procedure we outlined above. This time, however, select the This Computer Connects To The Internet Through A Residential Gateway Or Through Another Computer On My Network radio button at the beginning. Everything else is the same, and the only thing to keep in mind is that you must turn on the computer connected directly to the Internet before any of the other computers on the network can share the Internet connection.

If you make a mistake and accidentally assign the wrong setting to a computer (telling Windows it has the incoming Internet connection when it really doesn't or vice-versa), repeat the process outlined above and make the appropriate adjustments.

Software Troubleshooting

Problem: I want to play a multiplayer game with some friends on my home network, but it keeps asking me for each computer's IP address. When I go to Web sites that tell you your IP address, it comes back the same for each machine.

Solution: Every device connected to your network has a unique IP (Internet Protocol) address so the data intended for that device can be routed to it. The problem is that most routers use NAT (Network Address Translation) technology to assign unique IP addresses to devices on your home network but make only one IP address visible to the Internet. When you go to a Web site such as Your IP Is (www.whatismyip.com), it sees only what the router is telling it, and to play games or use other applications on your network, you'll need to determine the internal IP address assigned to each machine.

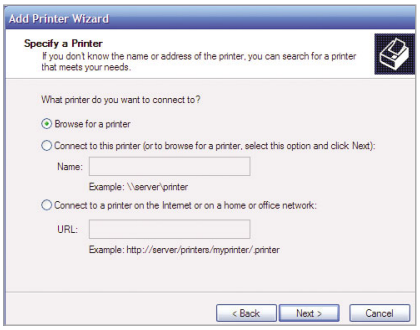
My computers are on a network, but only one of them has Internet access.

To do this in WinXP click Start and then Run, type **cmd**, and press ENTER. Type **ipconfig /all** and press ENTER; the number listed next to the IP Address entry is the one currently assigned to that computer. Repeat this for all machines, and remember that most routers assign IP addresses dynamically, so you may need to repeat this process in the future if you reboot the computers.

Problem: An online program or online game that I play worked fine when the broadband modem was connected directly to my PC, but after I installed a router (or a firewall), I could no longer connect to the game, regardless of which computer on the network I tried.

Solution: Information that flows to and from a router enters and exits via a series of numbered ports. For example, all POP (Post Office Protocol) email downloaded from your ISP's email server comes through port 110. The ports can be opened and shut, just like a door, and most routers come with the majority of the ports closed because each open port represents a security risk. **Firewalls**, which are programs designed to prevent unauthorized data from entering your computer from the Internet or exiting your computer to the Internet, also block many ports by default. Some online games and programs require that certain ports remain open in order to function, and if the newly installed router or firewall is blocking those ports, the program can no longer connect to the Internet.

The solution is **port forwarding**, where you manually open the appropriate ports; unfortunately, this is not an easy process. You must know exactly what ports to open, and then you must access your router and firewall settings to give those ports the green light. There are far too many routers, firewalls, and programs out there for us to provide specific instructions, but we can recommend the Port Forward Web site (www.portforward.com).

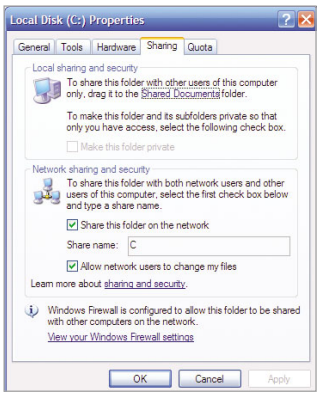

Add Printer Wizard
Specify a Printer
If you don't know the name or address of the printer, you can search for a printer that meets your needs.
What printer do you want to connect to?
Browse for a printer
Connect to this printer (or to browse for a printer, select this option and click Next):
Name:
Example: \\server\printer
Connect to a printer on the Internet or on a home or office network:
URL:
Example: http://server/printers/myprinter/.printer
< Back
Next >
Cancel

Network printers let everyone on the network print directly to them but only if they are configured properly.

The site has excellent lists of the ports that common programs use along with guides for specific makes and models of routers, so you can get your game or other software running again without having to sacrifice your network.

Problem: A program or wizard asked for my computer's network workgroup name, but I can't find it anywhere.

Solution: Every device that's connected to a Windows network has a workgroup name, which is just a label Windows uses to let you divide the network into different segments if you so desire. For example, a network might contain computers in a workgroup called "Team One" and other computers in a workgroup called "Team Two." Although those computers are all attached to the same basic network, they "see" only one another.


Local Disk (C:) Properties
General
Tools
Hardware
Sharing
Quota
Local sharing and security
To share this folder with other users of this computer only, drag it to the Shared Documents folder.
To make this folder and its subfolders private so that only you have access, select the following check box.
Make this folder private
Network sharing and security
To share this folder with both network users and other users of this computer, select the first check box below and type a share name.
Share this folder on the network
Share name:
C
Allow network users to change my files
Learn more about sharing and security.
Windows Firewall is configured to allow this folder to be shared with other computers on the network.
View your Windows Firewall settings
OK
Cancel
Apply

Sharing files using Windows XP is easy, but you should make sure your network is secure before doing so.

To find or edit the Workgroup name in WinXP, click Start, right-click My Computer, click Properties, and click the Computer Name tab. The name is listed to the right of the Workgroup entry. You should keep all workgroup names on your network the same, or the computers won't be able to see one another.

Problem: I want to save a file to another computer on the network, but I can't figure out how to locate the save location using the program's Save feature.

Solution: To save the file, open the File menu and click Save As instead of just clicking Save. When prompted for a location in WinXP, click the My Network Places icon on the left and navigate to the folder you want to save to on the other machine—just as you would on the machine on which you are working. Remember, the computer or NAS device you're saving to must be turned on for this to work.

Performance Issues

Problem: My router is flaky and often resets itself, fails to work well (or at all) with new networked devices I install, or suffers from other random outages.

Solution: Routers can fail just like any other piece of hardware, so if possible you should test the device on different router ports or get your hands on a different router to see if that's the problem. Also try replacing the Ethernet cable because they sometimes (albeit rarely) get damaged and fail.

Most often strange and random router behavior is caused by out-of-date firmware. **Firmware** is software that is semi-permanently installed on a special memory chip inside the router, and it defines what the router can do and how it does it. The nice thing about firmware is that although it remains when the router is turned off, you can replace it through a process called **flashing** that lets you update the

Wireless networks are much worse in terms of performance and often don't achieve even half of their rated speed.

memory chip with newer, better, and more efficient firmware. Firmware can do anything from fixing bugs to improving the router's speed or even increasing its wireless range. It's very important to check the router manufacturer's Web site every few months to see if updated firmware is available for your device.

The downside to firmware is that if the flashing procedure is interrupted, it can corrupt the memory chip and make it impossible to reinstall the firmware, turning the router into a big paperweight. Because of this, and because of the fact that wireless network connections are so spotty, always connect the router to a PC using an Ethernet cable and perform the flashing routine over the cable connection and not over the wireless connection.

Problem: My computer can't access the network at all, even though it is connected to the router.

Solution: Sometimes, rebooting your computer will get your computer and router talking again, but WinXP can serve as an intermediary if resetting doesn't work. Click Start, click My Network Places, and click View Network Connections. Click Local Area Connection (or the icon that corresponds to your NIC) and click Repair This Connection. This forces the router to re-recognize the PC and assign it an IP address along with some other important data that can get the connection up and running again. Click OK in the Repair Connection dialog box to dismiss it.

Performance Issues

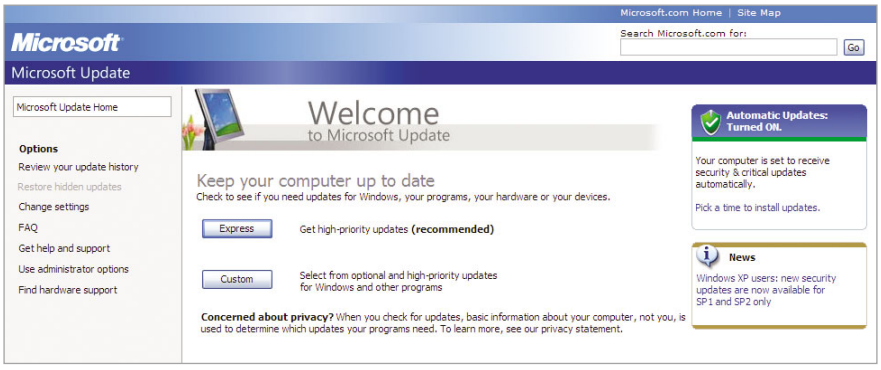
Problem: My network runs at a much lower speed than advertised.

Solution: Are you sure? A common mistake is to translate network speeds, which are measured in Mbps (megabits per second), into MBps (megabytes per second). There are eight megabits in each megabyte, so it should theoretically take about eight seconds to transfer 100MB worth of files across a typical 100Mbps wired network, or about a minute and 20 seconds to transfer 1GB of files across the same network.

Unfortunately, networks never live up to theoretical maximums. Wired networks suffer from network overhead that never lets them achieve true 10Mbps, 100Mbps, or 1Gbps (gigabits per second) speeds (depending on the hardware), although they get close. Wireless networks are much worse in terms of performance and often don't achieve even half of their rated speed.

Hardware mismatches compound the problem. If you have a router capable of 1Gbps speed but force it to communicate with NICs and other devices that operate at 100Mbps, data over the connection will never exceed 100Mbps, even though the router is advertised as having a speed of 1Gbps. Also remember that any speed-boosting technology your wireless router uses only works with devices on your network that use exactly the same technology the router uses and come from the same manufacturer as the router. Use it with something else and it defaults to the lowest speed both devices have in common.

If your network runs much slower than expected (for example, you have a 100Mbps wired network connection that never gets above 10Mbps in terms of data transfer speeds), the problematic device likely needs a setting adjustment. To do this in WinXP, click Start, click My Network Places, and click View Network Connections. Right-click Local Area Connection, click Properties, and, on the General tab, click Configure. Select the Advanced tab, click the Link Speed/Duplex Mode entry on the left (this may be labeled slightly differently depending on the NIC you use), and use the Value drop-down menu to select the NIC's highest possible speed. For example, if you have a NIC that operates at either 10Mbps or 100Mbps, select the 100Mbps/Full Duplex setting, or whichever 100Mbps setting your NIC offers (don't ever use half duplex). If you use a mix of networking hardware that all works at different speeds, you need to select the automatic (sometimes listed as Auto Detect, although the exact wording varies from NIC to NIC) Mode setting.


Microsoft.com Home | Site Map
Microsoft
Search Microsoft.com for:
Go
Microsoft Update
Microsoft Update Home
Options
Review your update history
Restore hidden updates
Change settings
FAQ
Get help and support
Use administrator options
Find hardware support
Welcome
to Microsoft Update
Keep your computer up to date
Check to see if you need updates for Windows, your programs, your hardware or your devices.
Express
Get high-priority updates (recommended)
Custom
Select from optional and high-priority updates for Windows and other programs
Concerned about privacy? When you check for updates, basic information about your computer, not you, is used to determine which updates your programs need. To learn more, see our privacy statement.
Automatic Updates: Turned ON.
Your computer is set to receive security & critical updates automatically.
Pick a time to install updates.
News
Windows XP users: new security updates are now available for SP1 and SP2 only

Keep Windows as secure and efficient as possible via Windows Update.

Problem: When I use a networked device to play video files over the network the resulting video is choppy or cuts out completely.

Solution: One of the benefits of having a fast home network is that you can use computers and certain other devices (such as a properly configured Xbox 360) to watch video being fed to it from the Internet or from another computer on the network. If you copy the video to the device on which you intend to play it (for instance, if you completely download a video file and then play it on a computer), the resulting video should be silky smooth as long as the PC has the proper hardware and software to handle playback. Often video viewed over a network is streamed, which means the file plays as it is being transferred over the network, meaning playback can begin almost immediately (you don't have to wait for it to finish downloading). The downside is that network glitches can interrupt the data stream and cause choppy playback, which you can learn more about in the Web-only "Network Video: Streaming vs. Downloading" sidebar (www.smartcomputing.com/extra/networking).

There are a few ways to improve streaming audio and video performance, and the best way is to use the fastest possible connection. A wired connection is always the most reliable (and usually the fastest), but if you're forced to stream multimedia wirelessly, always try to do so using devices that use the 802.11g or 802.11a wireless protocols instead of the older and much slower 802.11b protocol. Also remember that if your router supports 802.11a, 802.11b, and 802.11g, it will only communicate with a wireless NIC using the wireless NIC's protocol. You may need to upgrade to an 802.11g or 802.11a NIC to get smooth streaming multimedia performance.

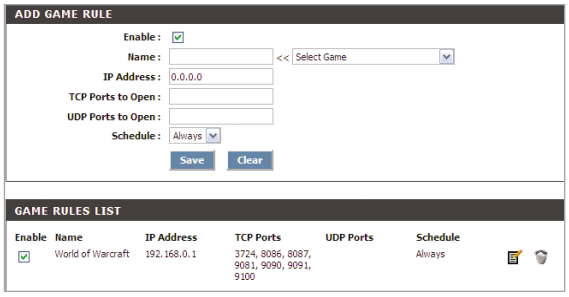
Network Setup Wizard
Welcome to the Network Setup Wizard
This wizard will help you set up this computer to run on your network. With a network you can:
• Share an Internet connection
• Set up Windows Firewall
• Share files and folders
• Share a printer
To continue, click Next.
< Back
Next >
Cancel

The Network Setup Wizard makes it easy to get all of your computers and network devices connected.

Problem: A program or my ISP is asking for my router, NIC, or broadband Internet modem's MAC address, but I have no idea where to find it.

Solution: For external devices you don't even need a computer to solve this dilemma. Pick up the router or modem, look for a sticker that has the MAC address printed on it, and write it down. The MAC address always contains six pairs of alphanumeric characters, and each pair is separated by a colon. Alternatively, you can access the router's configuration page using your Web browser (according to the instructions that came with the device) and look for a Device Info page or something similar that lists the MAC address.

If your MAC address is housed inside the computer, you'll need Windows to help search. In WinXP, click Start, click Run, type **cmd** in the text box, and click OK. At the DOS prompt, type **ipconfig /all** and press ENTER and you'll see the MAC address for the NIC in the Physical Address line.



If online games or other Internet-enabled applications give you trouble, solve it using port-forwarding.

Problem: My network connection is stalled out—files won't transfer, I suddenly can't see other computers, and every computer on the network has lost access to the Internet.

Solution: Routers, like any other computer hardware, sometimes malfunction due to software glitches or other problems. If it appears that the network isn't working, the quickest and easiest way to wake it up is to unplug the power cord from the back of the router, wait 10 seconds or so, and plug it back in. This restarts the router without erasing all of the settings you've established; you'll lose the settings if you use the reset button instead of cutting off the power.

If that workaround doesn't work, try restarting each computer and device attached to the network. If neither of those procedures works, you may have a hardware problem. If every device on the network has lost access, you may need to repair or replace the router. If only one device loses access and you can't get it reestablished, that device's NIC or Ethernet cable may be damaged; try swapping out the cable first and then the NIC and/or Ethernet cable if nothing else works.

Next Up: Wireless Woes

Although the tips in this article can help you recover from the most common wired network nightmares, you may be wondering why there's not much about wireless networks here. The answer is that wireless networks are so temperamental that we decided to devote an entire article to them in this issue. See the next article, "Wireless Woes," on page 138 for more information on wireless networks. RS

By Tracy Baker

Wireless Woes

Fixes For Wireless Network Problems

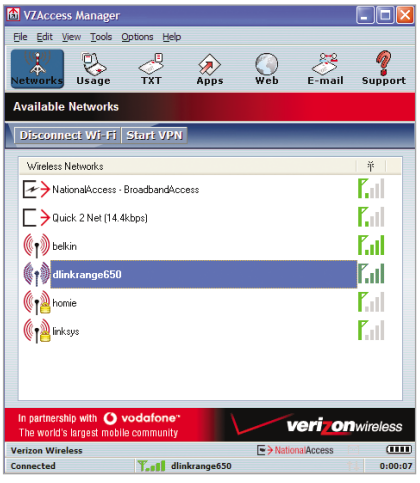
It always happens when you're in a hurry. That reliable 802.11g wireless network, the one you use in your home for easy Internet access and file-sharing from a laptop, suddenly loses its connection. You click the refresh button in Internet Explorer, and see nothing but an error message and a blank page. Call it the Murphy's Law of 802.11g. It's even stranger when your connection sputters and stalls for no apparent reason, or when you pop a PC Card into your Acer Aspire only to find that a driver is outdated or won't work with a Windows XP patch.

Wireless networks are mostly reliable and trouble-free. Designed for the home user and anyone who owns a laptop, 802.11g routers send out a signal across your entire home and help you avoid installing Ethernet cables to every room. Normally, once the network is running, you can connect easily every time. Yet, wireless networking sometimes runs into channel congestion and interference, and there's the occasional driver conflict or unchecked WinXP option. In this troubleshooting guide, we'll help you solve the most common issues that arise.

Q WinXP does not list any wireless networks in the Wireless Network Connection utility, but I know my router is running. How can that be?

A This is one of the most common—and confusing—problems when it comes to wireless networking. If you are using a laptop or desktop computer, and you know you have inserted a PC Card, enabled the wireless option on your laptop, or inserted a USB device that lets you connect to your home wireless router, you might find that you can't see your router name in the Windows Network Connection utility. This utility runs when you right-click the wireless network icon in your system tray, or click Start, Connect To, and Wireless Network Connection, to find your wireless network. The router name is also known as the SSID (Service Set Identifier).

In most cases, the reason you can't see any wireless networks listed is due to a driver issue. If you recently upgraded to a USB Wi-Fi key or a PC Card and installed a driver for it, then WinXP relinquishes the connection duties to that driver. It also means you most likely have an icon on the System Tray for that driver. You can double-click the icon and perform a wireless network scan, then connect to your router that way. Most drivers, such as the one that comes with many Linksys wireless networking products, will provide an option to use Windows Zero Configuration networking. Look for that checkbox in the driver, and select it. Then close the driver window. Now, use the Windows Network Connection utility again. You should see wireless networks listed. Another workaround is to just remove any wireless network drivers that you installed, perhaps by accident, on your computer. Just go to Start and Control Panel, run the Add Or Remove Programs utility, and remove any wireless network drivers.



The driver for a PC Card such as the one shown here will control your wireless connections instead of Microsoft's Windows Wireless Connection utility.

Q My wireless connection drops out repeatedly. Why can't my system maintain a connection?

A You can lose a wireless network connection for two reasons. The first reason has to do with wireless range. Most 802.11g routers provide about 300 feet in diameter of coverage indoors or 600 feet in diameter outdoors. So, if you are trying to connect in the living room, and your router is in the den more than 300 feet away, then you might be able to connect for short periods. The solution is to move your laptop or desktop PC closer to the router for a better signal. Newer 802.11n routers provide better coverage. For example, D-Link offers their RangeBooster DIR-635 router and

matching PC Card, the RangeBooster N 650 Notebook Adapter, for more like 1000 feet of range from the router. That's 2000 feet of total coverage, or more than enough for the average American home.

The second reason you can lose a wireless connection repeatedly is due to interference, even if connecting initially is easy and the router name (the SSID) is always available. The most common cause of interference is actually other wireless networks. See the sidebar on using NetStumbler to find out which channel you are using and adjust that option on your router to help with interference from other routers. Other wireless devices, such as portable phones, baby monitors, and even microwave ovens, can also cause interference. This issue works exactly like the channel button on your portable phone: You can usually push a channel button to clear up static on your phone, and you can do the same thing on your router.

An easier solution, though, is sometimes just to move your laptop computer to another location. If you're in a back office, try connecting from a bedroom. If you can maintain the connection, you know that there's a range or interference problem. You can then adjust channels or turn off interfering devices.

Q Why do I keep connecting to my neighbor's wireless network when I'm trying to connect to my own wireless network?

A WinXP has an amazing ability to manage wireless connections. If there is more than one network present, the operating system will actually search for and connect to the strongest wireless signal. Problem is, you may not want to connect to the strongest signal. To control how you connect, go to Start, Connect To, and Show All Connections. Right-click the wireless network icon and select Properties. Click the Wireless Networks tab. If you see multiple wireless network names listed, click the one that's yours and click Move Up until it is listed first.

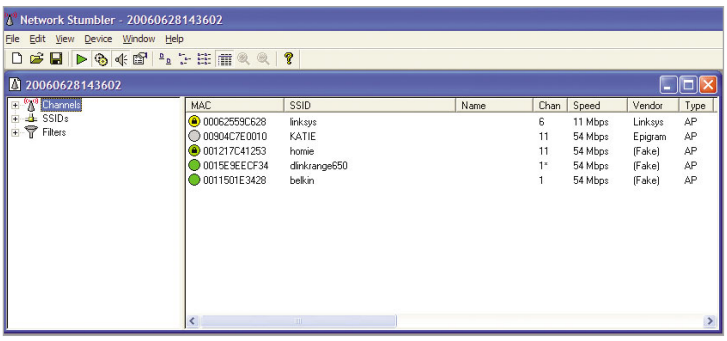
Another option is just to move your router closer to where you want to connect. That way, your router will emit the strongest signal and your laptop or desktop will connect first to that network.

Q When I insert the PC Card I use to connect to my wireless router, why does my computer either not recognize it or display an error message?

A Here's another common issue that is, fortunately, easy to rectify. This problem usually happens on laptops that use automatic battery management. Perhaps you changed a setting on your Dell Latitude to help save battery power when you are not connected to an electrical outlet. Power options are easy to access right from the WinXP system tray or from Control Panels. On most laptops, one power saving measure is to disable the PC Card port. So, when you insert a card, it won't receive power, and therefore won't let you connect wirelessly. The solution is to double-click the power icon in the system tray, or start the power control panel, and then change the settings so that the PC Card is not disabled when you are running on battery power.

Sometimes, an error message will appear when you insert a PC Card or USB device. In most cases, this is a simple driver conflict that you can resolve by rebooting the computer. WinXP sometimes (but rarely!) loses track of which devices are inserted on your PC.

In some cases, another cause for this issue is that you need to upgrade the driver for your PC Card or USB Wi-Fi adapter. Finding an update is easy: Just go to the Web site for the company that makes the device (such as Linksys), and then click Support. You'll need the exact model


Network Stumbler - 20060628143602
File Edit View Device Window Help
20060628143602
Channels
SSIDs
Filters
MAC SSID Name Chan Speed Vendor Type
00062559C628 linksys 6 11 Mbps Linksys AP
00904C7E0010 KATIE 11 54 Mbps Epigram AP
001217C41253 homie 11 54 Mbps (Fake) AP
0015E9EECF34 dlinkrange650 1* 54 Mbps (Fake) AP
0011501E3428 belkin 1 54 Mbps (Fake) AP

NetStumbler is a powerful tool for discovering which channel your neighbors are using for their wireless networks.

Use NetStumbler To Fix Wireless Network Problems

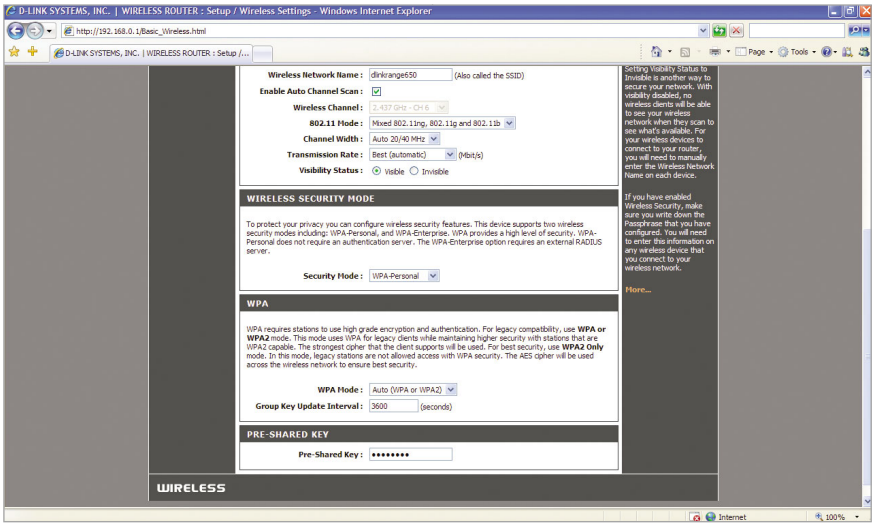
One way to resolve wireless networking problems is to change to a wireless channel that no one in your neighborhood is using. For example, if your router is set to channel 2, and your neighbor's is causing conflicts and interference because it is on the same channel, you can set your router to a different channel, such as 8, to make your network run smoother.

The only real trick is figuring out what channel your neighbor is using. NetStumbler, available for free at www.netstumbler.com, let you scan for competing wireless networks. You can then see which channel your neighbor is using. To change the channel used on your router, just run the installer program that came on the included CD. Most setup programs either provide a way to change the wireless channel, or at least a way to access the advanced features on the router. ❙

name, which is listed on the device. Every Web site works a bit differently, but you can usually search for or scroll through a list and find your particular product. Then, just download the driver and run the simple installer to upgrade to the new driver.

Q When I connect to a wireless network, why do I get an error message that says my laptop has "little or no network connectivity"?

A Anyone who has used wireless networking has probably seen this small balloon pop-up appear. Often, WinXP will display that message just for a moment as your PC is connecting to the network, and then after a moment you will be able to use the Internet and connect to another computer. If you see the error, and know you are connected to your router, and yet still can't access the Internet, then it's possible that your cable or DSL (Digital Subscriber Line) modem is disconnected from the router. Or, you may just need to reboot the router by unplugging the power connection, waiting about one minute, and then plugging it back in. On rare occasions, there is an IP (Internet Protocol) problem between your computer and the router. Rebooting both the router and your PC usually resolves those issues. If you happen to be running two wireless routers, connected by an Ethernet cable, and they are the same brand, then an IP conflict will occur. To solve that dilemma, contact the technical support for the router manufacturer to find out how to set a different IP range for one of the routers. This process varies by manufacturer.

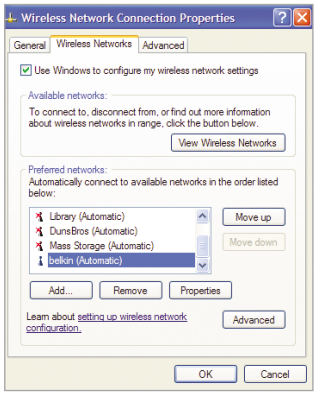


You can enable WPA security for industrial-strength encryption that's nearly unbreakable.

Q My wireless network is running unusually slow. I know it should run faster, so why doesn't it?

A It's easy to notice this problem if you normally can download files from the Internet quickly, or share files across the network in just a few minutes, and then find that these activities are running much slower than usual. The usual culprit is channel interference. Other wireless devices, such as a bay monitor or portable phone, can add signal noise to the wireless channel and make your connection run slow. The best solution is just to power down these devices so they do not interfere. Or, you move your router to a different location where there are no competing signals. Another approach is to just move your computer closer to the router.

Occasionally, a slowdown will occur if another user is connected to your network. It could be someone else in your home, but if a neighbor has attached and started downloading a bunch of massive movie files from the Internet, your network will certainly seem slow. The solution is to control who connects by enabling security. In most cases, you can just run the installer program that came with your router, which will walk you through the process of enabling security. You will type in a passcode that must be entered in order to connect. WinXP will request the passcode.



Windows XP lets you choose a preferred network, so that if other networks are present, you will attach to that network first before any others.

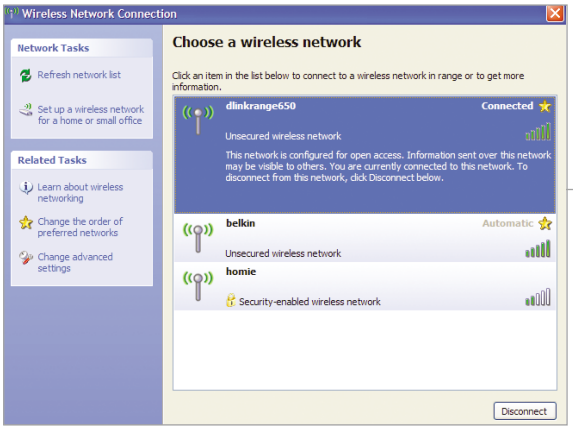
Q Why is there one room in my house where I am unable to connect to my wireless network?

A As we mentioned earlier in this guide, a common issue with wireless networking is that you can't quite connect because the 802.11g range is only 150-300 feet. If you just need to extend the signal to one more room in your home, the best option is to use an antenna booster. Hawking Technology (www.hawkingtech.com) makes several products that can boost a signal, some designed for your laptop and others for your router. You can even add a signal booster on both ends of the wireless signal for the best connection strength. The boost also helps make your network run faster, because a stronger signal moves data faster around your home.

Q Why can my neighbor connect to my network? His computer even shows up in my Network Neighborhood in WinXP.

A If you are running a wireless network and do not have security options enabled, then anyone can connect and use your Internet access, "borrow" files from your computers, install viruses, and just wreak havoc on your network. There's even a way hackers can install programs to log what you type (including credit card numbers) and make your computers unbootable.

Most routers offer some form of security encryption, which makes it difficult—if not impossible—for someone to gain unauthorized access to your network. Encryption such as WPA (Wi-Fi Protected Access) uses randomly generated passcodes that are continually updated so that no one could break the code. Older routers used WEP (Wired Equivalent Privacy) security, but this method is easy to crack using programs you can download from the Internet. You can enable security by running the installer program that came with your router and selecting the security option and typing in a passcode. Some passcodes are just a series of numbers; some are a hexadecimal code such as BC98BBDCC9 that is much harder for people to guess. WinXP will display a login screen on any computer trying to access your wireless network.


Wireless Network Connection
Network Tasks
Refresh network list
Set up a wireless network for a home or small office
Related Tasks
Learn about wireless networking
Change the order of preferred networks
Change advanced settings
Choose a wireless network
Click an item in the list below to connect to a wireless network in range or to get more information.
dlinkrange650
Connected
Unsecured wireless network
This network is configured for open access. Information sent over this network may be visible to others. You are currently connected to this network. To disconnect from this network, click Disconnect below.
belkin
Automatic
Unsecured wireless network
homie
Security-enabled wireless network
Disconnect

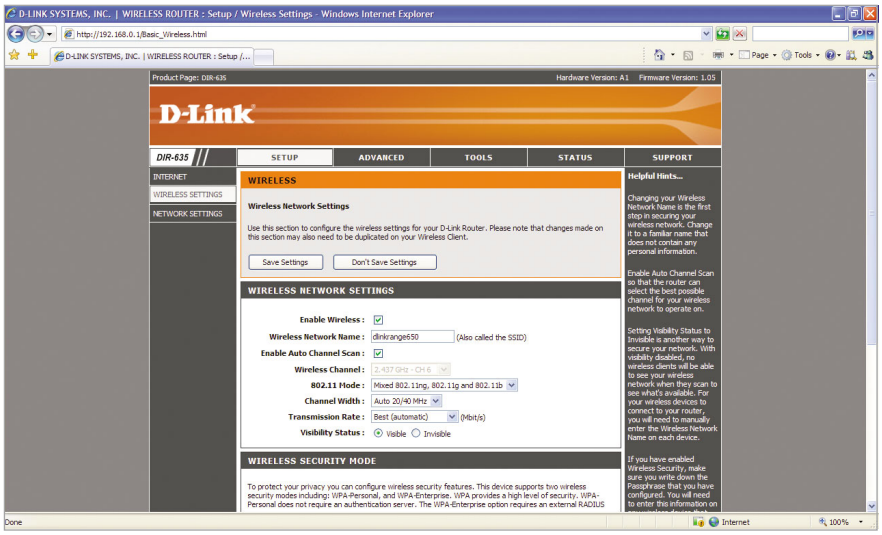
The Windows Wireless Connection utility allows you to connect to a wireless network. The utility comes with Windows XP Service Pack 2.

Other security methods are available. Buffalo Technology (www.buffalotech.com) makes routers that use a system they call AOSS (AirStation One-Touch Secure System). This means you can press a button on the router, and click another button in the connection program on your laptop, and enable security. Pure Networks makes Network Magic (www.networkmagic.com), a program that lets you configure security options for most popular routers using an intuitive interface.

Q Why won't my new 802.11n router work with my 802.11b/g USB adapter or with a PC Card?

A Newer routers such as the D-Link RangeBooster DIR-635 uses a much faster wireless technology that sends out three signals at the same time, running at about 120Mbps. Even the previous generation routers based on AirGo's True MIMO (multiple-input, multiple-output) Gen 3 technology were much faster than the original 802.11g products. Older wireless gear, including 802.11b USB adapters and some notebooks, might not support the latest routers, but there is an easy fix.

Most new routers provide a "compatibility mode." This means you can tweak the settings during setup, when you run the installer program, so that the router works with legacy devices. The only real issue is that, once in compatibility mode, the router can't operate at the lightning-fast speeds. Since 802.11n gear costs so much more than 802.11g, it might actually be more prudent to upgrade the client adapter than to run in a slower wireless networking mode.



Most routers support a compatibility mode so that you can access the router with an 802.11b, 802.11g, or newer 802.11n clients.

Get Back In Action

Most of the time, wireless networking works just fine. You can connect easily, and stay connected. When problems do arise, they are easy to solve by moving closer to the router, upgrading a driver, or tweaking some of the router settings. In no time at all, you can fire up your laptop again and start surfing the 'Net, even from the backyard patio. RS

BY JOHN BRANDON

Networking Snags In Windows XP

Troubleshooting Tips To Help You Get Up & Running Again

Thanks to the Network Setup Wizard (new with Windows XP), configuring and running a Windows network is easier than ever before. Furthermore, WinXP is more flexible than its predecessors. Not only does it let you create mixed-OS (operating system) networks, combining WinXP PCs with Windows 95/98/Me machines, but it also supports the combining of wired and wireless networks.

However, such automation and flexibility comes at a price. Like so many aspects of WinXP, an array of background operations and technologies work in concert to keep everything flowing smoothly. If you (or another service or program) install, disable, or reconfigure a component improperly, trouble won't be far behind. Throughout the next few pages, we'll provide solutions for some of the common problems you're liable to see while you are configuring and running a WinXP network. Note that all solutions assume you click OK or Yes as necessary to exit dialog boxes and windows after you complete a step. Additionally, some require you to use Control Panel in Classic View. (Select Control Panel from the Start menu and select Switch To Classic View.)

Problem: I used the network bridge feature to set up a combined wireless and wired network with three computers, but one of the computers isn't visible to the other two.

Solution: A network bridge lets a computer become a member of two networks with disparate connection types, forging a link between the two networks and effectively combining them into one. For best results, the bridging computer (the one with two network adapters) should be running WinXP Professional. Otherwise, the PC will act as a conduit but will not be a member of either network (and therefore not able to view the other computers). If you have WinXP Pro on another machine, install two adapters in that machine instead. WinXP should automatically sense the presence of the two adapters and create the bridge. (If not, use the same process you used before to create the bridge.)

If you do not own a copy of WinXP Pro, you may be able to work around this obstacle by mapping (assigning a drive letter to) the shared folders of the other computers on the network. (However, we should mention that this doesn't always work.)

Problem: Prior to running the Network Setup Wizard, several of my computers were sharing an Internet connection. Now, their Internet connections aren't working properly.

Solution: As part of the setup process, WinXP can enable ICS (Internet Connection Sharing) among all the computers (WinXP or earlier) on your network. However, ICS works differently in earlier versions of Windows such as Win98. Consequently, WinXP's Network Setup Wizard will sense earlier setups of ICS, but it will be unable to update them. Disable the existing ICS connections on all non-WinXP computers and rerun the Network Setup Wizard. For help disabling ICS in earlier PCs, go to Microsoft's Help And Support (support.microsoft.com) and search for article No. 230112.

Problem: I added another computer to the network, but it's not showing up in Network Places.

Solution: Any time you make changes to the network, you may need to rerun the Network Setup Wizard on all machines. If the new computer doesn't show up after you run the wizard, you can map (assign a drive letter to) the computer's shared drives or folders. To map a resource, select My Network Places from the Start menu. When My Network Places opens, open the Tools menu and select Map Network Drive. Click the Browse button to locate the resource or specify the resource manually in the Folder field. (Use two backslashes followed by the computer name, a single backslash, and the resource, such as \\familyroompc\music). The resource will then show up in My Computer as a drive you can open and explore.

If WinXP cannot find your new PC, it's possible there is a problem with the computer's hardware or network settings. Because these problems and their solutions can be complex, we won't delve into troubleshooting them here. Skip to "More Help" for additional suggestions.

Problem: After I installed my WinXP network, the only thing that showed up for each PC was a folder called Shared Docs.

Solution: By default, WinXP only shares the Shared Documents folder on each networked machine. This is a built-in security feature designed to prevent accidental erasure or alteration of important files. However, you can use the Simple File Sharing feature to share as many original folders as you wish with the members of your network. Users can access any open file in a shared folder, including a program if that's where you install it or place its shortcut.

Locate the folder on the computer that will share it; right-click My Computer on the Start menu and select Explore to get started. Next, right-click the folder and select Sharing And Security (Sharing on some machines). Click the Sharing tab. To let users read or copy to their machines (but not modify or delete the original), you need to select the Share This Folder On The Network checkbox.

To let users modify or delete your original files, you also need to select the Allow Network Users To Change My Files checkbox. Before you choose this option, consider that when a user deletes files from a shared drive, Windows bypasses the Recycle Bin and permanently deletes the files.

If you try to share an entire drive, WinXP will warn you that it is a risky decision because doing so makes your computer and network more susceptible to malicious intrusion. (Especially if you share your system drive.) Before you can share a drive, you must log in to an Administrator-level account.

Problem: When I share folders on the network, I don't see any options to set passwords for access or instill any other restrictions.

Solution: On most WinXP machines, a component called Simple File Sharing is turned on by default. Simple File Sharing is exactly what its name implies: very simple and not very secure. In WinXP Home, this is your only option. (Plan to upgrade the systems that share resources if you want more control.)

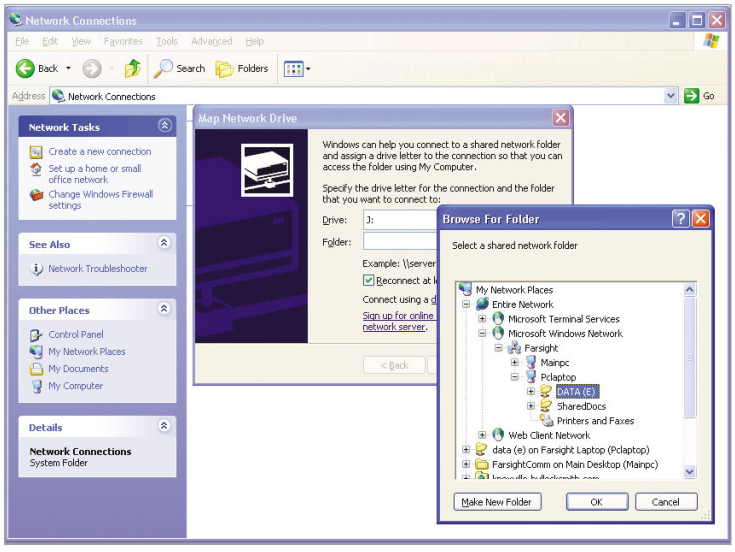
Fortunately, in WinXP Pro you can turn off Simple File Sharing and use a more robust access model. However, WinXP Pro still doesn't support password-protected shares as Win98 did. The only password is the one required at user login.

To turn off Simple File Sharing in WinXP Pro, select My Computer on the Start menu. On the Tools menu, select Folder Options, open the View menu, and deselect the Use Simple File Sharing (Recommended) checkbox. And then click OK. Note that turning off Simple File Sharing will not turn off the sharing of any previously shared resources.

Now, when you right-click a folder and select Sharing And Security, you'll see a different interface. Select Share This Folder and assign a share name (12-character maximum) and a comment (if desired). Click the Permissions button, and you can alter the access level for Everyone (all members of the network).

WinXP Pro also offers a single, more convenient interface from which you can add, delete, and change permissions for folders and drives. Right-click My Computer on the Start menu and select Manage. Click the plus sign (+) in front of Shared Folders to expand this option. Right-click the Shares folder and select New File Share to start the Create A Shared Folder Wizard. Click Next and browse to the location of the folder you want to share and click OK. After you assign a share name (and optionally, a share description), the wizard will prompt you to assign permissions. You can choose read-only access for all users, read-only access for all users but allow Administrators to modify or delete, or Administrator-only access. To edit permissions or stop sharing once you establish them, right-click the shared resource in the Sharing folder. Then select Stop Sharing to end resource sharing or select Properties to edit permissions.

There is no way in a workgroup environment to restrict certain folders to a particular user. However, you can



Drive Mapping makes shared resources on another network PC appear as a drive letter in My Computer and can provide access to computers and folders that would not otherwise appear on the network.

hide a shared folder by placing a dollar sign immediately after the share name. You can then give only authorized users instructions for locating it. (To access a hidden folder, the user must map it to a network drive, supplying the computer name and the folder name with the dollar sign appended.)

You can click the Customize Permissions radio button to establish more detailed restrictions. However, your options will be limited if you are not a member of a domain (a dedicated client/server network). If you need to restrict access by certain PCs you can modify a PC's security policy instead.

Problem: I've designated all the resources I want to share, but other network users either cannot access them or receive error messages.

Solution: A common reason for problems accessing network resources is that ICF (Internet Connection Firewall, WinXP's built-in software firewall) is not configured to allow network access. If during network setup you did not tell WinXP you planned to share files, it would have configured ICF to block incoming network traffic. If network members are having problems accessing shared resources, open Network Connections (click Connect To on the Start menu and select Show All Connections) on the PC they are trying to access and click Change Windows Firewall Settings under Network Tasks. Make sure Don't Allow Exceptions is deselected. Click the Exceptions tab and make sure the File And Printer Sharing checkbox is selected.

In some instances, depending on your configuration, you may have to turn off ICF for a user to access files. As long as you have ICF (or a more robust firewall solution) enabled on the PC that has a direct Internet connection, your entire network will enjoy that level of protection.

Problem: I understand that WinXP also has a feature that lets me prevent a specific user from accessing a particular computer, but I did not see that option in the various Sharing dialog boxes.

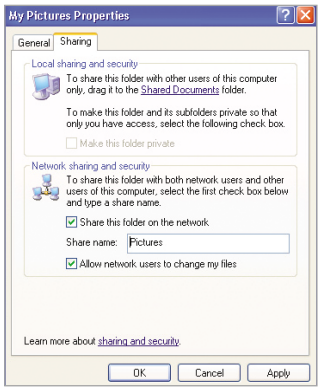
Solution: The ability to completely deny access to a particular user is not present in WinXP's default sharing component. Furthermore, WinXP Home has no capability for user-level control, and you will not have complete access to user-level security restrictions unless the computer is part of a domain. In many cases, you can walk through an entire process only to have WinXP Pro tell you the operation failed. However, on WinXP Pro machines with Simple File Sharing turned off, you can use Local Security Policy to restrict certain computers from connecting to them.

Select Control Panel on the Start menu and double-click Administrative Tools. Double-click Local Security Policy and click the plus sign to expand Local Policies. Click User Rights Assignment, and then double-click Deny Access To This Computer From in the right pane. In the resulting dialog box, click the Add User Or Group button, and then click the Locations button in the next dialog box. Select the workgroup name but not the local computer name. Click Advanced and then click Find Now. When WinXP returns the list of network computers, select the PC you want to restrict. You need to click OK several times to complete the process. This setting will override all other sharing settings. When someone on that computer attempts to access the restricted PC, he will see a message indicating "User has not been granted requested login type."

There is an array of permissions you can edit from this display, but be careful when making changes to ensure they are correct. For advanced information on security policies and access control, visit the Windows XP Professional Resource Kit online at www.microsoft.com/technet/prodtechnol/winxppro/reskit/default.mspx and select Managing Authorization And Access Control. (You might also want to review the Managing Files And Folders section.)

Problem: I turned Simple File Sharing on and now some of the resources I had previously shared are no longer available.

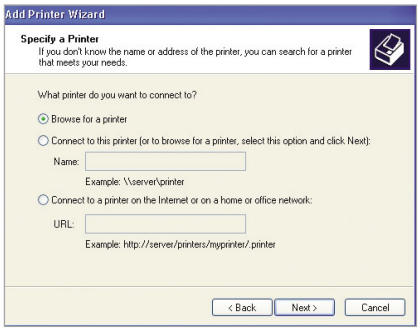
Solution: When Simple File Sharing is turned on, every user authenticates as Guest. Consequently, there are no Administrators. Any resource to which you assigned Administrator-only access will not be available for browsing under Simple File Sharing. You need to change the sharing settings to Everyone before other users can browse this resource.


My Pictures Properties
General
Sharing
Local sharing and security
To share this folder with other users of this computer only, drag it to the Shared Documents folder.
To make this folder and its subfolders private so that only you have access, select the following check box.
Make this folder private
Network sharing and security
To share this folder with both network users and other users of this computer, select the first check box below and type a share name.
Share this folder on the network
Share name: Pictures
Allow network users to change my files
Learn more about sharing and security.
OK
Cancel
Apply

In WinXP Home (and Win XP Pro with simple file sharing turned on), file sharing is a fairly simple yes or no proposition.

Problem: I installed a new network printer recently, but the other members of the network cannot detect the printer.

Solution: When you set up the network, WinXP should enable printer sharing automatically for all printers on the network. If you add a new printer later (or if an existing printer is for some reason not visible), make sure you shared the printer appropriately. From the Start menu of the machine where you installed the printer, select Printers And Faxes. Right-click the printer and select Sharing. Click the Sharing tab and ensure Share This Printer is selected. Note that you can click the Security tab and change permission settings as you can for folders.


Add Printer Wizard
Specify a Printer
If you don't know the name or address of the printer, you can search for a printer that meets your needs.
What printer do you want to connect to?
Browse for a printer
Connect to this printer (or to browse for a printer, select this option and click Next):
Name:
Example: \\server\printer
Connect to a printer on the Internet or on a home or office network:
URL:
Example: http://server/printers/myprinter/.printer
< Back
Next >
Cancel

WinXP's Add Printer Wizard enables network users to connect to new printers you add to the network.

If this doesn't resolve the problem, you can add the printer manually. For each computer on the network, select Printers And Faxes from the Start menu and under Printer Tasks choose Add A Printer. Follow the wizard to have WinXP browse for the newly added printer. Another option is to rerun the Network Setup Wizard on all network machines.

Problem: Every time I shut down one of my networked computers, I get a message to disconnect from the Internet even though I don't have my browser or email client open.

Solution: If you are using ICS, this behavior will occur if other users are browsing the Internet and you shut down the PC with the direct dial-up Internet connection. If you want users to be able to browse the Internet whenever they wish, you should leave the connected PC up and running whenever other users might need it. If not, you can instruct WinXP not to let other users control the connection.

In Network Connections (click Connect To on the Start menu and select Show All Connections), right click your Internet connection, select Properties, and click the Advanced tab. Deselect the Allow Other Network Users To Control Or Disable The Shared Internet Connection checkbox and click OK.

Problem: When I rebooted my computers after running the Network Setup Wizard, I saw a message that began "Duplicate Name Exists . . ." What does this mean?

Solution: If you accidentally give two PCs on your network the same name, WinXP will recognize the error. Because the name of each computer must be unique on the network, you will be unable to register the two computers on the network until you change one of the network names. To do this, right-click My Computer on the Start menu, select Properties, and click the Computer Name tab. Click the Change button and provide a new name.

Problem: I installed a wireless network but some of my machines cannot connect to the network.

Solution: WinXP offers a special Wireless Network Setup Wizard for wireless users. If you didn't use this when you installed your network, you should run it now. If you don't see it in Network Connections, select Help And Support from the Start menu, search for Wireless Network Setup Wizard, and select Setting Up A Wireless Network. You will then need to run the Network Setup Wizard if you want to share folders and printers.

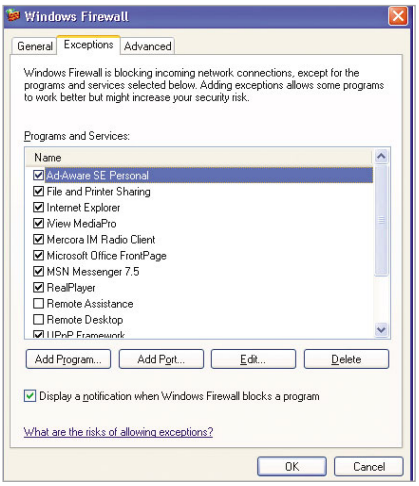
If you set up the network properly but one or more PCs cannot connect to the network, first make sure their access points are not too far from the PCs. If this doesn't solve the problem, you can configure the network manually. From the Start menu, select Connect To, and click Show All Connections. Right-click the wireless connection and select Properties. Click the Wireless Networks tab and, in the Available Networks area, click your network and click Configure. Using the instructions that came with your networking equipment, provide the SSID (Service Set Identifier), WEP (Wired Equivalent Privacy) encryption, and authentication settings for your network. If you are not using a wireless access point or router, set the network mode to Ad-Hoc.

If your network isn't listed as an available network, you can click Add to manually configure settings. When you save these settings, you can use them automatically when the network is available. You'll probably need to repeat this process across your network.

If you do not see a Wireless Networks tab (or cannot locate a wireless connection), the device driver is causing problems, most likely with WinXP's Wireless Zero Configuration service, the component that supports wireless networking. Visit the Microsoft Help And Support and search the Knowledge Base for article No. 313242. This article will walk you through the entire (sometimes lengthy) process of configuring your network adapters to work with WinXP.

More Help

For problems that go beyond the scope of our suggestions, check out WinXP's Network Troubleshooter.



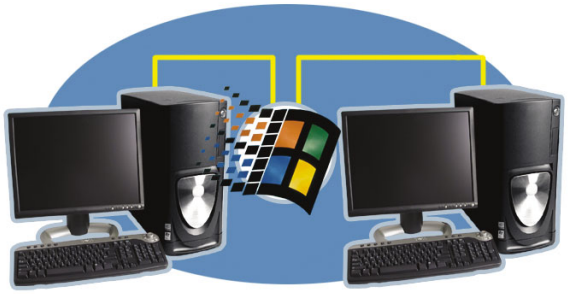
File And Printer Sharing must be enabled in ICF or the firewall will block network users trying to access your shared resources.

Select Connect To from the Start menu on a WinXP computer and choose Show All Connections. Next, select Network Troubleshooter under See Also. Microsoft's Help And Support Center appears, connecting you to a list of troubleshooting articles. RS

BY JENNIFER FARWELL

Stay Out Of Trouble

Solutions For Your Windows 98 Network Problems



Networking Windows 98 computers presents challenges you won't find when you network Windows 2000/XP machines. Microsoft based both Win2000 and WinXP on the Windows NT kernel—a foundation designed for networking. With Win98, despite the presence of networking software and utilities, you're dealing with a consumer-grade operating system not really built for use in a networked environment. We'll provide solutions (in likely chronological order) for some of the more common issues you may experience when creating and running a Win98 network.

Note that many of the solutions here begin in Control Panel or the Network dialog box. To open Control Panel, click Start, select Settings, and click Control Panel. To open the Network dialog box, double-click the Network icon.

Problem: I installed the NICs (network interface cards), but my machines don't recognize one or more of the cards.

Solution: If your NICs are Plug and Play (meaning Win98 will recognize them upon physical installation), Win98 may have walked you through the setup process. If this didn't happen, consult the documentation that came with the card to see if there is a special installation process. (Even with Plug-and-Play cards, it is best to follow the manufacturer's installation instructions, if there are any special ones.)

If not, you can use the Add New Hardware Wizard to install your NICs. (If your NICs were previously present but are missing from your configuration now, or if the solution that follows doesn't help, skip to the "Final Thoughts" section.)

In Control Panel, double-click Add New Hardware to start the wizard. Win98 will search for your card and prompt you to supply the media (a CD or floppy diskette from the manufacturer) with the device drivers .

If Win98 doesn't detect your NIC, you can install it manually (when you are offered the option, choose to locate in on a list). If that doesn't work, contact the hardware manufacturer of the NIC for further assistance.

Problem: I installed my Win98 network, but no computers are present in the Network Neighborhood.

Solution: Only PCs with something to share (a drive, folder, or printer) appear in Network Neighborhood. Other PCs are there, they just aren't making a contribution. If you haven't shared resources on computers within the network, you need to do so before they appear in Network Neighborhood.

If you set up shared resources on a PC and it still doesn't appear in the Network Neighborhood, check the Ethernet connection at the back of your PC and ensure the lights on the NIC are lit up. Also, eliminate sources of electrical interference, such as cordless telephones or radios, near your network cabling.

If everything looks good, check for the presence of Client For Microsoft Networks. This component must be on every PC in the network before it can access resources from another member of the network. Open the Network dialog box, select the Configuration tab, and look for Client For Microsoft Networks in the list. If your computer lists this item, you can name your computers. If you don't see Client For Microsoft Networks, click the Add button. (You may need your installation media to add this component.)

In the resulting list double-click Client. When the Select Network Client dialog box appears, choose Microsoft in the Manufacturer's list and double-click Client For Microsoft Networks in the Network Clients list.

To share resources on this PC, you also need a file-sharing component. Repeat the steps above, looking instead for File And Printer Sharing For Microsoft Networks in the list on the Configuration tab. After you click the Add button, skip to the next problem in our list ("There is no Sharing option on my drives or folders") before exiting. Otherwise, click OK as necessary to exit the display and restart your PC.

Problem: There is no Sharing option on my drives or folders.

Solution: To share files you need File And Printer Sharing For Microsoft Networks installed and enabled on each sharing PC. Open the Network dialog box, click the Configuration tab, and look for File And Printer Sharing For Microsoft Networks in the list. If you do not see it, click Add. You may

need your installation media to add this component. In the resulting dialog box, double-click Service, select File And Printer Sharing For Microsoft Networks from the Models section, and click OK.

Click the File And Print Sharing button and select one or both checkboxes (to share files, printers, or both). Click the Access Control tab; Share-Level Access Control should be selected. Click OK as needed to exit the dialog boxes and restart your PC.

If your networking component files are corrupt, file sharing will not be an option. If the solution above does not resolve your problem, follow the instructions in the previous solution ("I installed my Win98 network, but no computers are present in the Network Neighborhood") and this solution, only in reverse (click Remove instead of Add), restart the computer, and reinstall the networking components.

Problem: I turned on File And Printer Sharing in the Network dialog box, but my computers still don't appear in Network Neighborhood.
Solution: In addition to enabling your networked PCs to share information, you must choose which resources to share. (Repeat this process for every shared PC.)

Right-click the drive or folder in Windows Explorer, select Sharing, and click the Sharing tab. (If this option is not present or grayed out, refer to the previous problem: "There is no Sharing option on my drives or folders.") Select Shared As and create a name for the shared item. Then choose an access type: Read-Only (users can only view or copy to their PC), Full (users can edit, overwrite, and delete), or Depends On Password (access is dependent on the password the user supplies).

You can (and should, if your network is connected to the Internet) create passwords no matter which access type you select. Using Depends On Password is a great way to restrict some users to read-only access while giving others more control.

After you set up sharing for a drive or folder, a hand icon appears beneath it on-screen. To stop or change resource sharing, return to the Sharing tab and select Not Shared or change the access level as desired.

Problem: After I enabled file sharing and attempted to browse the network, I got a message that said "Unable To Browse The Network."
Solution: Most likely, you tried to browse too quickly after turning everything on. In a Win98 network, the network software automatically selects a Browse Master, one PC of the bunch that acts as an electronic "crossing guard." This can take a few minutes. However, if after waiting a few minutes you still cannot browse, try disabling the Browse Master selection on all machines and assign one PC as the Browse Master.

Add New Hardware Wizard
This wizard searches for new drivers for:
PCI Ethernet Controller
A device driver is a software program that makes a hardware device work.
< Back
Next >
Cancel

If Win98 doesn't install your NICs automatically, the Add New Hardware Wizard may help.

On each machine, open the Network dialog box, select File And Printer Sharing For Microsoft Networks on the Configuration tab, and click the Properties button. On the Advanced tab of the resulting dialog box, select Browse Master from the Property list and select Disabled from the Value drop-down menu, and click OK. Shut down all computers on the network. Next, Restart the newest computer with the most recent version of windows and return to the File And Printer Sharing For Microsoft Networks Properties dialog box. Select Enabled from the Value drop-down menu to make this computer the Browse Master. Reboot this machine and all others, and wait about 45 minutes for the computers to find the Browse Master.

Problem: I've done all the steps to share files, but some of my shared PCs are still not appearing in Network Neighborhood. Any suggestions?
Solution: Every computer on a Win98 network must have a unique computer name and should have the same workgroup name. If you have already assigned appropriate computer and workgroup names, see "Resources that I previously used are now not appearing in Network Neighborhood."

If your computers are not showing up in Network Neighborhood, check the computer and workgroup name for each missing computer. From Control Panel, double-click the Network icon. Select the Identification tab in the resulting dialog box and enter values for the two names (no spaces; maximum 15 alphanumeric or special characters) and restart the PC. A computer description is not required.

If you assign the same computer name to two PCs, Windows will recognize that fact (if both PCs are connected to the network) and generate an error message. If this happens, use the instructions listed here to make the necessary changes.

Problem: Resources that I previously used no longer appear in Network Neighborhood.
Solution: For a number of reasons, Win98 will sometimes lose, or fail to find initially, a computer in the Network Neighborhood. You can search for the computer manually. (You'll need to repeat this process for all missing computers and repeat it on all PCs where resources are not visible.) If Win98 reports it cannot locate the computer after performing the following routine, run through the previous problems and solutions in this article.

From the Start menu, select Find, and then click Computer. In the Find

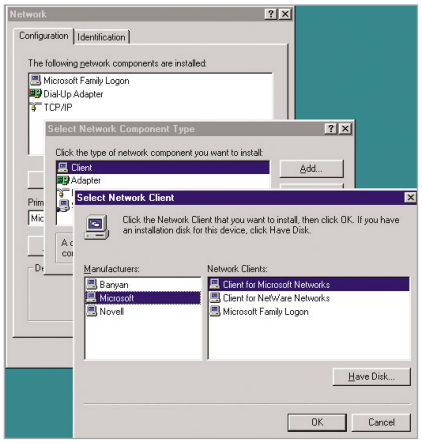
Computer dialog box, enter the computer's name in the Named field and click Find Now. If Win98 finds the computer, you can double-click the name to explore it.

You can also perform an operation called Mapping that will add an icon for the resource to the My Computer window and make it easier for you to locate should problems arise again. Right-click Network Neighborhood and click Map Network Drive. Assign a drive letter or accept Win98's suggestion. In the Path field, type ***\\computername\sharename***, replacing *computername* with the name you assigned the computer and *sharename* with the shared folder you want to map. Click the Reconnect at Login checkbox and exit the dialog box.

Problem: I installed a network printer on one of my PCs, but it's not in the Printers folder of my other machines.
Solution: Sharing a printer requires you to enable the same components and resources as sharing a file. Check that File And Printer Sharing For Microsoft Networks is installed and enabled. Next, make sure you have designated the correct resources to share. (From the Start menu, select Settings and then Printers. Right-click the Printer and click Sharing.) You can password protect a shared printer just as you can a shared file.

For a printer to show up in the Printers folder, you must also run the Add Printer Wizard. In the Printers dialog box, double-click Add Printer. In the second dialog box, select Network Printer. Provide the network path of the printer -*\\computername\sharedprintername*. (*Computername* is the name you gave the PC during setup and *sharedprintername* is the name of the printer on the network.) Continue through the wizard, giving the printer a name (for your use only) and printing a test page if you wish.

If you don't know the computer name or shared printer names, leave the wizard. To determine the computer name, open the Control Panel, double-click Network, and select the Identification tab. For the shared printer name, open Network Neighborhood, double-click Entire Network, and then double-click the name of your workgroup. Double-click the icon for the computer with the printer, and then locate the printer. You can also access the printer this way.



Adding Client For Microsoft Networks to every PC on your network ensures they can browse the other network members.

Problem: I want to configure user-level control for my Win98 network, but a dialog box appears with the following: "Obtain List Of Users And Groups From."
Solution: Win98 supports user-level access rights to other computers on the network only if the PCs are part of a domain (a dedicated client/server network) where another PC is a designated security server—a network member whose user list forms the basis for access control. However, if you have a WinXP computer, you can set up a mixed Win98/XP network from that machine and gain a little more control over user rights.

Problem: I purchased a wireless router and installed wireless cards into all my PCs, but the new system doesn't recognize my network.
Solution: Win98 can support wireless networking, provided you configure the router and cards properly using the instructions you received. However, if you were rushed and simply changed all the connections, having a pre-existing network is not enough.

Additionally, your new wireless router may use protocols other than the ones you used previously. Before installing your new wireless components, go to the Network dialog box and delete all components except Client For Microsoft Networks, TCP/IP, and Microsoft File And Printer Sharing. Then follow the instructions that came with your wireless router and cards for installation.

If you already installed the components properly and the network is not working, deleting these extraneous components may help. You may also need to contact the manufacturer or troubleshoot the hardware itself.

Final Thoughts

We don't have space to discuss advanced network troubleshooting procedures to resolve hardware failure, device conflicts, and system or file corruption. Fortunately, Microsoft offers two excellent support articles on these topics in its Knowledge Base. If the suggestions we provide here don't help, visit support.microsoft.com. Query article No. 192534 (general connection issues) and No. 133240 (device conflicts—when network hardware is missing or generating error messages).

However, in both these articles, Microsoft recommends you reconfigure device conflicts yourself. For less-than-advanced users, there may be an easier solution. If, while you are running through the suggestions in these articles, you find yourself in the Device Manager utility with a hardware conflict, delete the hardware and let Win98 try to resolve the problem before you proceed. From within Device Manager, select the hardware, click Remove to delete the hardware, and restart your PC. If this doesn't work, proceed with the instructions Microsoft provides. RS

BY JENNIFER FARWELL

Do It Yourself

Troubleshooting Network Problems In Windows Me

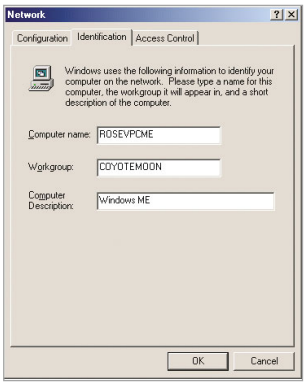
Networks may be ubiquitous, but they are far from being trouble-free. Fortunately, fixing many network problems does not require much more than a little information and some willingness to investigate.

We will primarily explore networking problems associated with Windows Me, but don't overlook the physical components (cables, power adapters, modems, printers, routers, and switches) that may make up your network. The reason you can't print to a shared printer in another room may be as simple as an unplugged device. Eliminate the simple fixes first; it doesn't take long, and it can save you from wasting time on a wild goose chase.

Troubleshooting Basics

Once you eliminate basic hardware problems, you need to consider software issues, especially drivers, which are pieces of software code that devices use to talk to a computer. WinMe includes a Network Diagnostic tool that runs a series of self tests and then presents the results. To access the Network Diagnostic tool, click Start and then select Help. When the Microsoft Help And Support window opens, click the Home Networking link. Click Troubleshooting For Networks and then click Using Network Diagnostics. The Network Diagnostics page will open and automatically start the diagnostic test. When it finishes, you will see the Status change to Finished. Click the Expand All button to view the results of the tests.

The Network Diagnostics tool starts by testing basic networking services, including a Loopback test. If the test passes, then Windows is able to talk to your NIC (network interface card). This means that the Windows-to-NIC interface works and that your NIC's driver software is also working. But that doesn't necessarily mean that the NIC can talk to any other device. The test goes on to ping your DNS (Domain Name Server) and your default gateway router, as well as the NIC's external IP (Internet Protocol) address. If your system passes these tests, you can rest assured that your NIC, as well as your basic networking services, DNS, and router, is working. If the Loopback and NIC IP tests pass, but the other tests (DNS and gateway router ping) fail, then you can reasonably assume that your computer and NIC are functioning, but that there may be a problem with the physical network components or the way they are configured.



Computer and Workgroup names must conform to specific naming conventions. Use uppercase letters and a maximum of 15 characters, with no spaces or special characters.

Check the IP address reported by your NIC in the Network Diagnostic test, under the Modems And Network Adapters section. If the IP is 169 .254.xxx.xxx , it indicates that your computer was unable to be assigned an IP from a DHCP (Dynamic Host Configuration Protocol) server, either on your network or from your ISP (Internet service provider).

The Network Diagnostic tool can help you pinpoint the problem. Look for the entry for DHCP Server or Default Gateway. For most home networks, these will be the same network device: your router. The tool will list an IP address and the result of pinging the address. If this test passed, then your computer can talk to the default DHCP server and/or default gateway. If this test failed, you will need to investigate the connection between your computer and the DHCP server or gateway, as well as confirm that the DHCP server is working correctly. For most home networks, the DHCP server and the router are one and the same, so consult your router manual for basic configuration and troubleshooting information.

The last important test to check is the results of the DNSServerSearchOrder. This test pings your DNS server's IP address, which is usually located remotely on the Internet. If your system passes this test, you know that you can access your DNS server as well as host computers on the Internet. Failing this test could indicate a problem with your ISP's network. Contact your ISP to resolve the problem.

Successful completion of the Network Diagnostics test ensures that your computer is able to communicate with your NIC and that your NIC can communicate with devices on your network and the Internet. At this point, you have successfully eliminated most hardware and driver issues as the cause of your network problem.

Networking Services

WinMe include services that make it easy to access and use your home network, including file and printer sharing. These services run as a peer-to-peer network, meaning no centralized server is necessary. Instead, each computer on the network can make services such as file sharing available to other devices on the network. In order for Microsoft's peer-to-peer network to work correctly, you must ensure the following.

1. Computer names on all networked computers must be unique. If two computers share the same name, or a computer's name doesn't conform to Microsoft's naming conventions, then file and printer sharing will not work correctly. For utmost compatibility, use computer names that contain no spaces or special characters. Also, use all uppercase letters, and limit names to a maximum of 15 characters. To check or change a computer's name, click Start, and select Settings, Control Panel. Double-click the Network icon. In the Network control panel, click the Identification tab. If needed, enter a new unique or conforming name in the Computer Name field. Click OK and restart your computer.

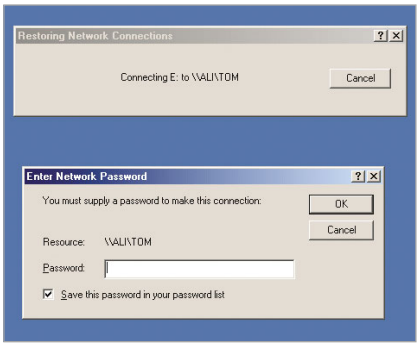
2. Workgroup names on your network should all be the same. To ensure the easiest network operations, workgroup names should be a maximum of 15 characters, and include no spaces or special characters. WinMe will automatically convert all letters to uppercase, but it's a good idea to enter the name in uppercase characters to begin with, to ensure uniformity with all present and future Windows OSes (operating systems). To check or change your computer's Workgroup name, click Start, and select Settings, Control Panel. Double-click the Network icon. In the Network control panel, click the Identification tab. Windows 9x/Me /2000 use WORKGROUP as the default workgroup name; Windows XP uses MSHOME as the default workgroup name. You can assign a name of your choice, such as your family name or a pet's name, as long as all computers share the same name. Click OK and restart your computer.

3. Use TCP/IP (Transmission Control Protocol/Internet Protocol). This is the preferred protocol for home networks. Windows OSes older than WinXP can use different protocols, including NetBEUI (NetBios Extended User Interface), an older, Microsoft-developed protocol for peer-to-peer networking. WinXP and later OSes do not support NetBEUI, so use TCP/IP instead. Click Start and select Settings and then Control Panel. Double-click the Network icon. In the Network control panel, click the Configuration tab. Select any NetBEUI entries and click Remove. You should now have only TCP/IP listed for your Ethernet Adapter and/or Dial-Up Adapter. Select the TCP/IP entry for your Ethernet adapter and click Properties. In the TCP/IP Properties window, click the Bindings tab. Make sure that Client For Microsoft Networks is checked. There may be other items in the Binding list, depending on what services you are running. Leave any other entries as they are. Click OK and then click the NetBios tab. There should be a check mark next to I Want To Enable NetBios Over TCP/IP. Click OK.

If your Ethernet adapter is not listed, you will need to reinstall its drivers. Refer to the Ethernet network card's instructions for assistance.

File Sharing

File And Printer Sharing is the most often used network service in any home network system. When it is working, you can access shared folders using My Network Places or by using mapped network drives via the Desktop or the Windows Explorer interface.



When your Windows login password and the password required to access a shared item aren't the same, you will be asked to provide the correct password.

When it is not working, problems range from cryptic error messages to a lack of shared items displaying in My Network Places, as well as a lack of access to shared printers.

Start with the basics. Is File And Printer sharing turned on for the device you want to access? It's not uncommon for individuals to turn these services off when they are using a computer for processor- or graphics-intensive applications, such as games or video-editing. In many cases, restarting the Sharing option will fix the problem. On the computer that hosts the shared folder, click Start and select Settings and then Control Panel. Double-click the Network icon. Select the Configuration tab and click File And Printer Sharing. Put a check mark next to the type of access you want to activate (files or printers). Click OK, click OK again, and then restart the computer.

While you're at the host computer, take the time to ensure that the folder you want to access is actually marked for sharing. Right-click the folder and select Properties from the pop-up menu. Click the Sharing tab. Make sure the Shared As option is selected, and that a Share Name has been

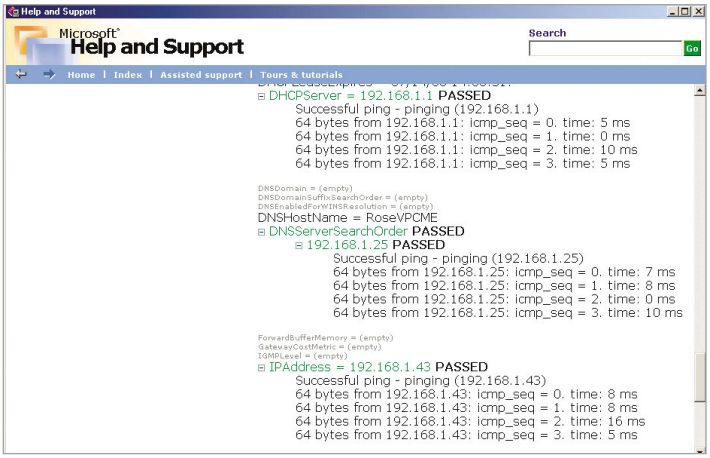
entered. Confirm that the Access type is configured for your needs (Read-Only, Full, or Depends On Password), and click OK.

File Sharing Security

File sharing security uses a simple shared-level access control that controls access based on how each resource is configured (read-only, full access, password dependent). With shared-level access, there is no concept of users. Everyone is essentially a guest and can access the available resources as long as they know the password.

The inability to access a shared resource is almost always a password issue. The most common problem is the ability to access some shared resources and not others. When you connect to a shared resource, Windows uses your Windows logon password. If it's the same as the resource's password, then you can connect without any trouble. But if the shared resource password differs from your Windows logon, an error message will prompt you to access the share with a different password. Entering the correct password should do the trick.

If you routinely access a shared folder, consider mapping it as a network drive. This allows the folder to appear to your computer as just another hard drive. You can configure your computer to automatically mount the network drive whenever you boot. To map a shared folder as a network drive, first access the shared folder. Double-click the My Computer icon and select Tools and then Map Network Drive. The Map Network Drive dialog box will display the first available drive letter not already in use. You can accept the suggested drive letter or select another from the Drive drop-down menu. To set the path to the shared folder, click the arrow in the Path drop-down menu. All shared folders you have accessed should display. Select the path to the shared folder you want to map as a network drive. If you want the folder to always be available, put a check mark next to Reconnect At Logon.


Help and Support
Microsoft
Help and Support
Search
Go
Home | Index | Assisted support | Tours & tutorials
DHCPServer = 192.168.1.1 PASSED
Successful ping - pinging (192.168.1.1)
64 bytes from 192.168.1.1: icmp_seq = 0. time: 5 ms
64 bytes from 192.168.1.1: icmp_seq = 1. time: 0 ms
64 bytes from 192.168.1.1: icmp_seq = 2. time: 10 ms
64 bytes from 192.168.1.1: icmp_seq = 3. time: 5 ms
DNSHostName = RoseVPCME
DNSServerSearchOrder PASSED
192.168.1.25 PASSED
Successful ping - pinging (192.168.1.25)
64 bytes from 192.168.1.25: icmp_seq = 0. time: 7 ms
64 bytes from 192.168.1.25: icmp_seq = 1. time: 8 ms
64 bytes from 192.168.1.25: icmp_seq = 2. time: 0 ms
64 bytes from 192.168.1.25: icmp_seq = 3. time: 10 ms
IPAddress = 192.168.1.43 PASSED
Successful ping - pinging (192.168.1.43)
64 bytes from 192.168.1.43: icmp_seq = 0. time: 8 ms
64 bytes from 192.168.1.43: icmp_seq = 1. time: 8 ms
64 bytes from 192.168.1.43: icmp_seq = 2. time: 16 ms
64 bytes from 192.168.1.43: icmp_seq = 3. time: 5 ms

The Windows Me Network Diagnostics tool checks many of the key elements of your network, include your IP (Internet Protocol) address, DHCP (Dynamic Host Configuration Protocol) server address, and DNS (Domain Name Server) addresses, to ensure that they are reachable and working correctly.

The failure to connect to a mapped network drive at startup is usually caused by—you guessed it—the wrong password. Your Windows logon password may not be the same as the password required for the mapped network drive. You can instruct WinMe to use a different password when connecting to mapped drives. Reboot your computer. WinMe will attempt to connect to any mapped network drives. If you cannot connect because of a password error, WinMe will display a dialog box that prompts you to provide the correct password. Enter the correct password and put a check mark next to Save This Password In Your Password List. In the future, WinMe will provide the correct password for the mapped drive.

Printer Sharing

If you can no longer print to a shared network printer, start with the simple things. Is the printer turned on? Is the host computer also turned on, with File And Printer Sharing enabled? If the answer to these questions is yes, check to see if you can access other shared resources on the host computer, such as a folder. If not, there may be a problem with the network connection. Follow the troubleshooting tips above, starting with the basic physical wiring.

If this is the first time you are attempting to use a network printer, make sure it is set up correctly on both your computer and the host computer. The printer must first be configured normally, as a local printer, on the host computer. After confirming that the host computer can access and use the printer, the printer can then be set as a shared resource. On the host computer, click Start, and select Settings and then Printers. Right-click the printer and select Sharing from the pop-up menu. Click the Shared As button and enter a name for the printer. You can also enter a password, but avoid this if possible, because some Windows OSes have trouble connecting to a password-protected shared printer. Click OK.

On your computer, use the Add Printer wizard to set up a new printer. Click Start and select Settings and then Printers. Click the Add Printer icon and follow the on-screen instructions. Be sure to select Network Printer as the type of printer to install.

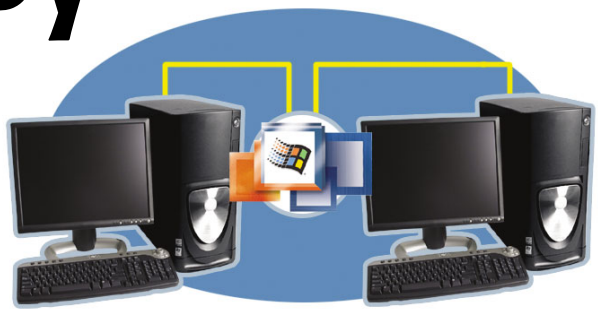
The Perks

Troubleshooting network problems may not be as much fun as tackling a home repair project, but it's a lot less messy. RS

BY TOM NELSON AND MARY O'CONNOR

Keep Your Network Happy

Tips For Fixing Your Windows 2000 Networking Problems



Windows 2000 and home networking were made for each other. Well, Win2000 was actually originally targeted to business users, but it excels as a working member of a home network. It has advanced security features, user permission options, and tools that can help you keep your network humming.

Before tackling the OS (operating system) side of the networking equation, check the physical components (cables, power adapters, modems, printers, routers, and switches) that make up your network. If you can't access a printer in another room, it certainly could be an OS issue, but it could also be as simple as a disconnected cable. Save yourself time and trouble, and eliminate the obvious possibilities first.

Troubleshooting Basics

Most Win2000 diagnostic and troubleshooting tools operate from the command line. To access the command line, click Start and then select Run. In the Run dialog box, type **cmd** and click OK or press ENTER.

To determine whether Win2000 can talk to your computer's NIC (network interface card), perform a basic loopback test. Bring up the command line, type **ping 127.0.0.1**, and press ENTER. When the test results display, the ping statistics should show 4 packets sent, 4 packets received, and no packets lost. Any other response indicates a problem with your NIC, or with the drivers that allow Win2000 and your NIC to communicate. Check the NIC manufacturer's Web site for updated drivers. Install the updated drivers and run the test again.

If you still have problems, try pinging your NIC's IP (Internet Protocol) address. To do this, you must first determine what that address is. Bring up the command line, type **ipconfig**, and press ENTER. The command result will list your NIC's IP address, Subnet Mask, and Default Gateway. Using the listed IP address, perform another ping test. You should once again see a response with all packets sent and received, and no packets lost. If there are any lost packets, disconnect the Ethernet cable from your NIC and perform the ping test again. If there are no lost packets this time, then the Ethernet cable or the network device to which the cable connects is having problems. If the ping test continues to fail, you may have a bad NIC. Replace the NIC and check your networking connectivity again.

If your NIC passes with flying colors, but you're still having problems, reissue the ipconfig command, and check the IP address it reports. It should be a valid IP, either manually assigned by you or automatically assigned by your router. If the IP is 169.254.xxx.xxx , it indicates that your computer was unable to be assigned an IP from a DHCP (Dynamic Host Configuration Protocol) server, either on your network or from your ISP (Internet service provider). You can try to force a new IP assignment from your DHCP server. Bring up the command line, type **ipconfig /release**, press ENTER, and then type **ipconfig /renew**. After you issue the renew command, the command results will list your IP address, Subnet Mask, and Default Gateway. If you still do not receive a valid IP address, check how your DHCP server is configured. In most cases, your DHCP server is your router. If so, check the instructions for your router to confirm that it is configured correctly and operating correctly. If your ISP supplies your DHCP service, contact your ISP for assistance.

The last test is to ensure that you can access your DNS (Domain Name System) servers. To do this, you need to know your DNS IP addresses. Bring up the command line, type **ipconfig /all** and press ENTER. Look through the results for a DNS Servers entry; there may be multiple IP addresses listed. Use the command line to issue a ping command for each IP address. The results for each should be the same as other ping commands; all packets sent, and no packets lost. If your system passes this test, you know that you can access your DNS server

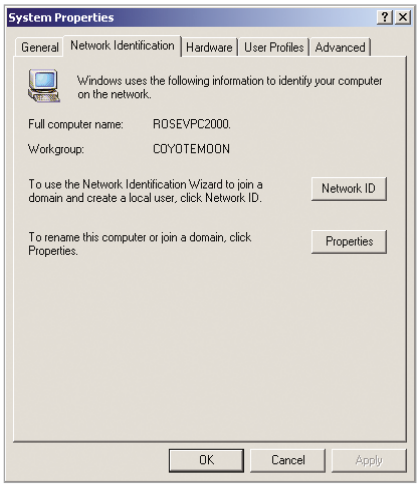
as well as host computers on the Internet. If your system fails this test, it can indicate a problem with your ISP's network. Contact your ISP to resolve the problem.

Successful completion of the above series of tests ensures that your computer can communicate with your NIC, and that your NIC can communicate with devices on your network and the Internet. At this point, you have successfully eliminated most hardware and driver issues as the cause of your network problem.

Network Services

Win2000 includes many services that make it easy to use a home network. We will concentrate on the basic File And Printer Sharing services. These services run as a peer-to-peer network, meaning no central server is necessary. Instead, each computer on the network can make services, such as file sharing, available to other devices on the network. In order for Microsoft's peer-to-peer network to work correctly, you must ensure that computer and workgroup names conform to specific Microsoft naming conventions. Computer names must be unique; no two computers on your network may have the same name. On the other hand, workgroup names must be the same. Computer and workgroup names should both be all uppercase letters, with no spaces, no special characters, and no more than 15 characters in length.

To check or change your computer's name, right-click the My Computer icon on the Desktop, and select Properties from the pop-up menu. Click the Network Identification tab to see your Computer and Workgroup names. Click the Properties button. If needed, enter a new name in the Computer Name field. In the Member Of area, make sure the Workgroup option is selected. Win9x/Me/2000 use WORKGROUP as the default workgroup name; WinXP uses MSHOME. You can assign a name of your choice, as long as all computers use the same name. Click OK and reboot.



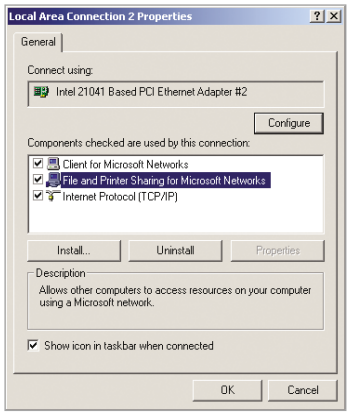
Every computer name on your network must be unique, but every computer you want to access on your network must share the same workgroup name.

File And Printer Sharing

File And Printer Sharing is used more than any other service in most home networks. When it is working, you can access shared folders through My Network Places, or by using mapped network drives, via the Desktop or the Windows Explorer interface. When it isn't working, you may see cryptic error messages, or you may notice that no shared items display in My Network Places, or that you can't access shared printers.

As always, start with the basics. Is File And Printer Sharing turned on for the device you want to access? Someone may have turned this option off when using another computer for processor- or graphics-intensive applications, such as games or video-editing. In many cases, restarting the Sharing option will solve the problem. On the computer that hosts the shared folder (or printer), right-click My Network Places and select Properties from the pop-up menu. Double-click the icon for your Local Area Connection and click Properties. Make sure that File And Printer Sharing For Microsoft Networks is listed and has a check mark next to it.

While you're at the host computer, verify that the folder you want to access is actually marked for sharing. Right-click the folder and select Properties from the pop-up menu. Click the Sharing tab. Make sure that the Share This Folder option is selected, and that a Share Name has been entered. Click the Permissions button to view the Share Permissions and make any necessary adjustments.



You must enable File and Printer Sharing before you can create shared resources on your computer.

Security

Win2000 has a wide range of security features that affect how a user, or group of users, can make use of a computer. The security capabilities that involve permissions, rules, and policies, both at the Active Directory level and local group levels, could fill a book or two. (In fact, they have.) Here, however, we are concerned with the use of local users and groups to allow simple peer-to-peer file sharing using Microsoft's built-in network clients.

These simple user security settings can cause unexpected problems when you attempt to access a shared folder or printer from other Windows computers on your network. The most common error starts with a dialog box that asks for a password in order to access a shared folder or printer. You provide a known good password, but it is

rejected, and you are asked to re-enter the password. The reason for this error is that Win2000 expects both the username and password to match up to a user defined in Users And Groups. When you attempt to access

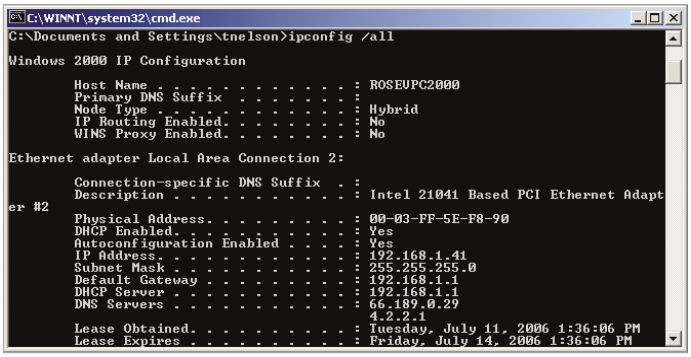
When you try to access a shared resource, Windows 2000 will expect both a username and a password.

a share, your currently logged in username and password are sent to the Win2000 computer that is hosting the share. If the username and password don't match up, Win2000 asks for another password but not another username. Even if you provide the correct password, your computer may not be supplying the correct username.

To fix this issue, make sure that any individual you want to have access to a share on a Win2000 computer is given a local username and password on that computer. You must log on to the host computer as an Administrator to make the following changes. Click Start and then select Settings and Control Panel. Double-click the Users and Passwords icon. Click the Users tab, and click Add. Enter a username that matches the Windows logon name on the remote computer (the one that will be used to access the computer that hosts the share). Click Next. Select a type of account for the user. Remote users usually do not need to be Administrators or even Standard users. For simple file access and printer sharing, selecting Restricted user will work nicely. Click Finish.

Another common error is, "*<share name>* is not accessible. Access is denied." This error message can crop up when the computer that hosts the shared folder or printer, or the printer itself, has been turned off or when there's a physical network problem.

Another common problem that can produce this error are shared item security settings that do not allow access for a particular user. This is a bit different than a share's permissions; it is the folder's permissions on the host machine. To correct this error, log on to the host computer with an account that has administrator privileges. Right-click the problem folder and select Properties from the pop-up menu. Click the Security tab, and scan the list of names to ensure that the individual's username, or a group the individual belongs to, is listed. If neither is listed, click the Add button. Scroll through the list of Users and Groups until you find the individual's username or a group the individual belongs to. Highlight the name, click Add, and then click OK. (Remember, if you select a group, you are giving all members of that group access to the files in the folder.) Back in the Security tab, highlight the name you just added to the list. The Permissions box will display the rights of that user to access the folder. For general read/write access, there should be a check mark in the Allow column next to Read & Execute, List Folder Contents, Read, and Write.


C:\WINNT\system32\cmd.exe
C:\Documents and Settings\tnelson>ipconfig /all
Windows 2000 IP Configuration
Host Name . . . . . : ROSEVPC2000
Primary DNS Suffix . . . . . :
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No
Ethernet adapter Local Area Connection 2:
Connection-specific DNS Suffix . :
Description . . . . . : Intel 21041 Based PCI Ethernet Adapter #2
Physical Address. . . . . : 00-03-FF-5E-F8-90
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
IP Address. . . . . : 192.168.1.41
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.1.1
DHCP Server . . . . . : 192.168.1.1
DNS Servers . . . . . : 66.189.0.29
4.2.2.1
Lease Obtained. . . . . : Tuesday, July 11, 2006 1:36:06 PM
Lease Expires . . . . . : Friday, July 14, 2006 1:36:06 PM

The Ipconfig /all command can provide important information about your network connection, including your DNS (Domain Name System) and the DHCP (Dynamic Host Configuration Protocol) servers you are using.

Printer Sharing

If you can't access a shared printer that you could previously access, and you've eliminated the obvious possibilities, there may be a network problem. Follow the troubleshooting tips listed above.

If this is the first time you've attempted to access a network printer, make sure that it is set up correctly, both on the host computer and the computer you are using to access it. On the host computer, the printer should first be configured normally, as a local printer. It must also have drivers installed for all of the operating systems that will be used to access it. On the host computer, click Start and select Settings and then Printers. Right-click the printer you want to share and select Properties from the pop-up menu. Click the Sharing tab, then click the Shared As button, and enter a name for the printer. Click the Additional Drivers button. Put a check mark next to any of the listed OSes you will use to access the printer and click OK. Follow the on-screen instructions to install any missing drivers.

On the computer you are using to access the shared printer, use the Add Printer wizard to set up a new printer. Click Start and select Settings and then Printers. Double-click the Add Printer icon and follow the on-screen instructions. Be sure to select Network Printer as the type of printer you wish to install.

Is Everybody Happy?

When your network is happy, then everyone in your networked world will be happy. All it takes is a little information and a willingness to look under the hood. RS

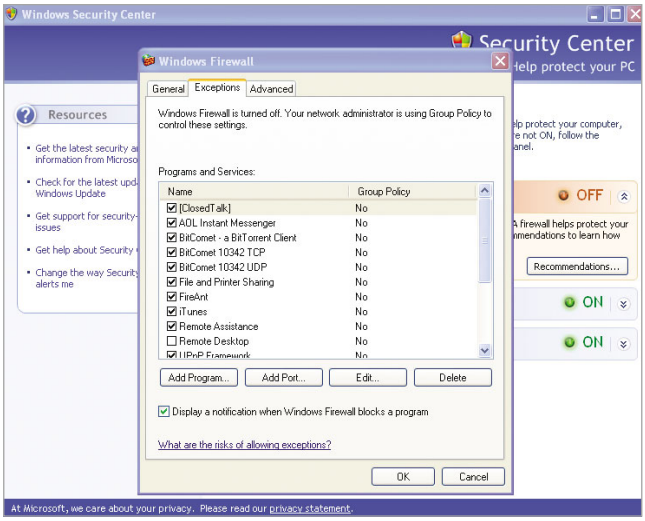
BY TOM NELSON AND MARY O'CONNOR

Long-Distance Runaround

Troubleshooting Remote Access Problems

Like a good road warrior, you set up your GoToMyPC or LogMeIn remote access accounts before leaving on your latest business trip. You should be all set to work on your home or office desktop from anywhere, right? But here you are, coffee in hand, in a lonely hotel room trying to log in and grab that file you left behind, and—nothing. What happened? Here are a few tips for keeping your remote access connections up and running efficiently.

For our examples we used the very popular Citrix, GoToMyPC (www.gotomypc.com), and the free version of LogMeIn (www.logmein.com). There are too many possible remote access services to review here, but many of these principles for connectivity and performance optimization apply to many other similar services. Note that when we use the term "host" in these tips, we are referring to the home/office-based computer on which the client software always runs. The "remote" computer refers to the PC or laptop that is connecting to your host via the remote access service.



Remote access programs often collide with system firewalls, which are designed to prevent exactly the type of behavior these services provide.

Problem: I am trying to install remote access software on my host PC, but it is not connecting to the online remote access service.

Solution: Most remote access solutions use client software that must stay active in order to reach out to the Web-based service. Security firewalls on the host PC can block this activity and mistake your client software for some sort of spyware or virus activity. In this article we are assuming your PC has Windows XP Service Pack 2 installed and that it's using only WinXP's built-in firewall protection. If you have a third-party security suite, such as Norton Internet Security (www.symantec.com) or the McAfee Internet Security Suite (us.mcafee.com), make these adjustments within those programs.

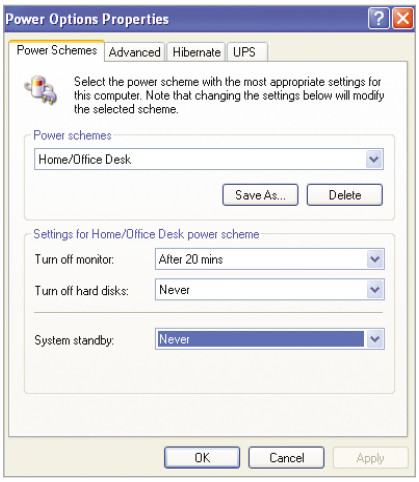
To ensure that your firewall allows the access client to contact the Web, open your Control Panel and double-click Windows Firewall. If the On radio button is selected in the General tab of the Windows Firewall dialog box that appears, click the Off radio button and then click the OK button below. Now try connecting the client software to the host again. If you succeed this time, then you know it is a firewall issue, so proceed to the next step.

Bring the Windows Firewall dialog back up and click the On radio button and then OK so as not to leave your PC unprotected. Next, Click the Exceptions tab. The Programs And Services window lists programs your firewall allows direct contact with the Internet. Use the Add Program button and browse the Programs list for GoToMyPC or whatever remote access client you have installed. Click the appropriate program listing, then click OK in this and any other open dialog boxes. Windows Firewall should now let the client connect to the access service.

For LogMeIn, as well as some other remote access clients, the program's name will not be a visible option in the program list in Windows Firewall's Exceptions tab. In that case, you need to locate the actual program files. Use the Add Program button and then in the next window the Browse button. Navigate to the Program Files folder on your primary hard drive (usually the C:\ drive) and open the LogMeIn subfolder. Click LogMeIn.exe to highlight it and then OK to add it to the Exceptions list. Now, use the Browse button again, click LogMeInsystray.exe, and click OK to bring that into the Exceptions list.

Again, click OK in any open windows to close it out.

Once you have entered these exceptions, you will need to reboot the system or reload the client software. Keep in mind that this basic principal of registering exceptions holds true with most third-party firewalls, as well. If you bring up the firewall details in such programs as Norton Internet Security, McAfee Internet Security Suite, or ZoneAlarm Internet Security Suite, there should be some obvious place for you to add programs that the firewall and other security measures allow to operate freely.



To keep a host computer awake and ready to accept remote access, you may need to block your PC from falling into sleep modes.

Problem: I have added my remote access client software to my firewall's list of exceptions, and the client software still cannot connect to the Web-based access service.

Solution: If your firewall is set up properly to allow remote access, then the blockage most likely is coming from your router, situated between your cable/DSL (Digital Subscriber Line) modem and your PC. The steps to create exceptions on a router are very specific to each model, so we can't outline them all here. You will need to consult your router's documentation for specific instructions. The best way to diagnose a connectivity problem as router-related is to unplug your broadband connection from your router and run it directly into your PC. If the client software now can connect to the access service, then you know that adjustments need to be made to the router.

Problem: I logged onto my remote service's Web site but it says my home PC is "offline" or unavailable.

Solution: Once this happens, there is not a lot you can do to bring your host PC online from a remote location. It is possible that while you were away a system conflict stopped the resident client software from running, so having someone at home or the office reboot your PC could reload the client software and establish the connection. More likely, your home PC slipped into a sleep or hibernation mode that is not waking up when GoToMyPC or LogMeIn tries to contact it from the Web. To ensure that the host PC is always available to the remote service, you may want to disable some of the power-saving features. For instance, right-click on any open area of the host PC's Windows Desktop and click Properties. In the dialog box that appears, click the Screen Saver tab and then click the tab's Power button. Generally, letting your system turn off the monitor or hard drives after certain periods of inactivity will not deter a remote access program from waking up the PC from afar. But if you are having trouble accessing the host remotely, then try selecting Never in the System Standby drop-down menu. Click OK to activate the change. Your system may also be set up to go into hibernation mode, which essentially turns the PC off after a certain period of inactivity and certainly will make it unavailable to remote access. To make sure this doesn't happen, click the Hibernate tab, deselect the Enable Hibernation checkbox if it contains a check mark, and click OK.

Problem: The remote access client software icon is not showing up in my System Tray and the host PC doesn't seem to be connecting to the remote access service.

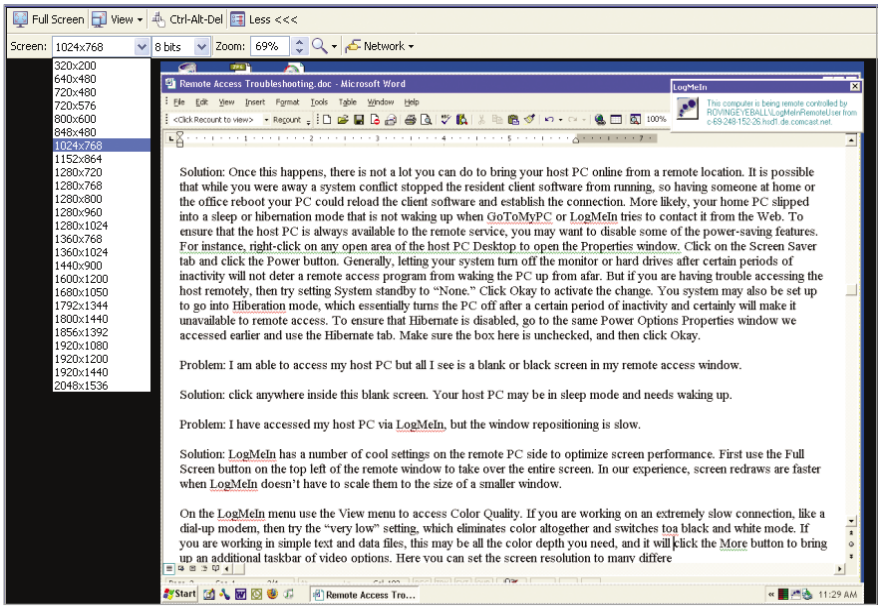
Solution: The client software on your host PC either has been disabled by a conflicting program or it is not loading properly when Windows boots up. If your firewall software warned you your access client was trying to access the Internet and you gave it the wrong response (if, for example, you told it to deny the program access every time it tries to connect), this may prevent the client software from loading properly at startup. If you are running a third-party Internet security program, it will detect when new installations of remote access programs force Windows to load something new at startup.

To see whether the remote access program is loading when you boot your system, click Start and then Run, and type **msconfig** in the Open field and click OK. This brings up the System Configuration Utility dialog box. Click the Startup tab to see a list of programs that launch on your system at startup. The checked items are the programs that Windows loads whenever it starts. If you are using GoToMyPC, look for the program named "g3svc." For LogMeIn, look for "LogMeInSystray." If you use Avvenu, the item you're looking for will be called "Avvenu." If the relevant item is unchecked, then for some reason Windows stopped loading it at boot. Click the checkbox next to the item and click OK to close the window. The program will ask whether you want to restart the PC now or wait until later. When you restart, Windows will load the client software properly.

If you did not find the remote access software listed in the Startup tab, it was most likely not properly installed to begin with. Try reinstalling the client software.

Problem: I am able to access my host PC but all I see is a blank or black screen in my remote access window.

Solution: Click anywhere inside this blank screen. Your host PC may be in sleep mode; you need to wake it up.


Full Screen
View
Ctrl-Alt-Del
Less <<<
Screen: 1024x768
8 bits
Zoom: 69%
Network
320x200
640x480
720x480
720x576
800x600
848x480
1024x768
1152x864
1280x720
1280x768
1280x800
1280x960
1280x1024
1360x768
1360x1024
1440x900
1600x1200
1680x1050
1792x1344
1800x1440
1856x1392
1920x1080
1920x1200
1920x1440
2048x1536
Remote Access Troubleshooting.doc - Microsoft Word
LogMeIn
Solution: Once this happens, there is not a lot you can do to bring your host PC online from a remote location. It is possible that while you were away a system conflict stopped the resident client software from running, so having someone at home or the office reboot your PC could reload the client software and establish the connection. More likely, your home PC slipped into a sleep or hibernation mode that is not waking up when GoToMyPC or LogMeIn tries to contact it from the Web. To ensure that the host PC is always available to the remote service, you may want to disable some of the power-saving features. For instance, right-click on any open area of the host PC Desktop to open the Properties window. Click on the Screen Saver tab and click the Power button. Generally, letting your system turn off the monitor or hard drives after certain periods of inactivity will not deter a remote access program from waking the PC up from afar. But if you are having trouble accessing the host remotely, then try setting System standby to "None." Click Okay to activate the change. You system may also be set up to go into Hiberation mode, which essentially turns the PC off after a certain period of inactivity and certainly will make it unavailable to remote access. To ensure that Hibernate is disabled, go to the same Power Options Properties window we accessed earlier and use the Hibernate tab. Make sure the box here is unchecked, and then click Okay.
Problem: I am able to access my host PC but all I see is a blank or black screen in my remote access window.
Solution: click anywhere inside this blank screen. Your host PC may be in sleep mode and needs waking up.
Problem: I have accessed my host PC via LogMeIn, but the window repositioning is slow.
Solution: LogMeIn has a number of cool settings on the remote PC side to optimize screen performance. First use the Full Screen button on the top left of the remote window to take over the entire screen. In our experience, screen redraws are faster when LogMeIn doesn't have to scale them to the size of a smaller window.
On the LogMeIn menu use the View menu to access Color Quality. If you are working on an extremely slow connection, like a dial-up modem, then try the "very low" setting, which eliminates color altogether and switches toa black and white mode. If you are working in simple text and data files, this may be all the color depth you need, and it will click the More button to bring up an additional taskbar of video options. Here you can set the screen resolution to many differe
Start
Remote Access Tro...
11:29 AM

Many remote access services like LogMeIn (pictured here) let you tweak performance by reducing the screen resolution on the host PC.

Problem: I can access my host PC remotely, but my apps run very slowly.
Solution: Any open programs or browser windows that communicate with the Web, whether on the host or remote PC, can seriously degrade the performance in your remote access window. On the host PC, close or suspend any programs such as file sharing or download clients (BitTorrent clients and the like) or antivirus or antispyware scans that may be occurring in background. On the remote PC, close all other browser windows, email programs, system scans or file downloads. If you are in the habit of watching DVDs or listening to music while working, close your multimedia programs down, as well, as they are notorious system resource hogs.

Problem: I have closed all other active programs, but things still seem to be running very slowly.
Solution: The easiest way to speed up remote access performance is to reduce the color depth of the window on your remote PC. In GoToMyPC, for instance, use the Tools menu to bring up the Preferences window. From the remote PC you will see this window come up on your host PC in the remote access window. The changes you make here, however, will affect how the host appears when you access it remotely.

Go to the Quality tab and click the radio button for 256-color mode. This will noticeably reduce the visual quality of the remote access window but it also substantially reduces the amount of visual data that the service must pass to your remote PC. In GoToMyPC, you can also click and drag the Performance slider to the left. This disables much of the unnecessary visual data being sent from the host PC, like the wallpaper background and animated transitions when moving windows.

Another way to improve responsiveness is to reduce the resolution on your host PC so that less screen information needs to be passed to the remote PC. Right-click the Desktop of your host PC (you can do this from the remote access window, as well). Click Properties and then click the Settings tab. If your resolution is set above 1,024 x 768, then bring the slider down to that resolution and click OK. If given the Compatibility Warning screen, select Apply The New Display Settings Without Restarting and then click OK. This will dial the screen resolution down. We have even tried going lower, to 800 x 600 on the host PC to get even better speed.

If you are only working on basic office tools like word processing, email, or spreadsheets, then the visual quality and color depth of the host PC are probably irrelevant to your work, but they will improve performance noticeably.

LogMeIn has a number of cool settings on the remote PC side to optimize screen performance. First use the Full Screen button in the top left of the remote window to take over the entire screen; screen redraws tend to be faster when LogMeIn doesn't have to scale them to the size of a smaller window. Click LogMeIn's View menu and then click Color Quality. If you are working on an extremely slow connection, like a dial-up modem, then try the Very Low setting, which eliminates color altogether and switches to a black-and-white mode. If you are working in simple text and data files, this may be all the color depth you need. For more granular control over a remote Desktop, you can also click the More button to bring up a taskbar with additional video options. Here you can choose among many resolution settings and reduce the color depth all the way to 4-bit, which redraws the screen very quickly but with only a few colors.

Problem: The video window to the host PC looks distorted or has odd visual artifacts.
Solution: You may need to resize the screen on the remote PC or change the color depth on the host PC.

In the remote PC's GoToMyPC window, click View and try switching between Actual Size and Scale To Fit to see if that does the trick. Also make sure the screen is set to 100% in the Zoom To submenu. Click Tools and Preferences, then try some of the same procedures we used to lower the color depth. In LogMeIn, click View to try the Actual Size and Fit To Window settings to find the best performance. RS

BY STEVE SMITH

Networking Terms To Know

adapter address—See "Ethernet address."

application server—Software running on a server whose purpose is to make available other software applications across a network. The result is more efficient use of RAM and CPU resources, with program access monitored and maintained by the Network Administrator.

backbone—The central cable that serves as a major communications conduit. This can be anything from world.com to a small cable connecting a few network-based devices, depending on the size of the network involved.

backdoor—An undocumented method of gaining entrance to a computer system. These are often placed in networks by programmers for easy troubleshooting, but hackers are especially good at sniffing them out.

bandwidth—Synonymous with "data transfer rate," and representing the maximum amount of information that can be carried between two networked points in a given span of time. It's usually measured in bits, kilobits, or megabits per second (bps, Kbps, Mbps). A 56.6Kbps modem, for example, is capable of delivering 56,600 bits per second, while a 100Mbps Ethernet adapter can deliver roughly 1 million bits per second. Note, however, that most bandwidth measurements are theoretical maximums, and that generally users experience data transfer rates that are lower than the given specification for a network, adapter, or other data transfer device.

biometrics—Security technology based on the recognition of unique physical attributes. Instead of requiring a password, network access may require a retinal scan, voice pattern match, or a fingerprint scan.

bridge—A device connecting either two LANs (local-area networks) or two segments of a LAN. Bridges forward packets without analyzing content and taking other action. This makes them less versatile than routers, but potentially more adaptable.

client—A networked computer that runs a client process. That process contacts the server and initiates requests. There are specific client programs for most server-side applications.

client-server network—As opposed to a peer-to-peer network, a client-server network connects at least one designated server (a computer that provides a networked service) with at least one client computer (service requester and recipient). The server typically provides a variety of services, including file sharing, network security, email access, Web access, printing, etc.

cracker—Some hackers insist that their efforts at breaking into networks are motivated by curiosity alone. They prefer to use the term "cracker" to identify someone who breaks into network systems with malicious or criminal intent.

data transfer rate—See "bandwidth."

DHCP (Dynamic Host Configuration Protocol)—A communications protocol that is similar in effect to the Bootstrap Protocol, but more sophisticated in design. Among other important differences, it can base network configuration data on geographical information rather than a client computer's unique Ethernet Address. This in turn allows a network to recognize a client computer continuing identity despite moves between several physical locations.

domain name—Not to be confused with host name, a domain name is assigned and registered by a domain name registration authority. As with the host name, it's usually mnemonic. Yourdomain.gov would be an example of a domain name that's part of a government-based organization.

encryption—The act of encoding data to render its contents unreadable without a proper code key, or the presence of such encoding.

Ethernet address—Also known as an adapter address, an Ethernet address is the basic address of an Ethernet network adapter, a 12-digit, 48-bit unique number. You can determine your Ethernet address by opening a DOS command prompt window, then typing **ipconfig/all** (or **winipcfg** in Windows 98/Me) and pressing ENTER. The address is always a hexadecimal alphanumeric value or series of alphanumeric values, such as 005035873E5C.

exploit—To exploit is to take advantage of a weakness; so in network security terms, an exploit is an attack designed to take advantage of a vulnerability in the system. Often, this vulnerability is a backdoor.

file server—A networked computer that supplies connected client computers with access to shared storage.

firewall—A protective network wall that blocks access without authorization. This can work both ways: A firewall can keep network users in as well as other users out, or limit access on either side.

forum—A subject-based network discussion group, or area. A given forum may be moderated, or have limited access.

gateway—The point on a network where hardware and software create the entryway to another network. This enables computers using a variety of protocols to interact properly. Gateway nodes for many corporations also fulfill the functions of firewall and proxy servers.

groupware—Network-based application software designed to allow simultaneous access to a group of users.

hacker—Someone who "hacks" a network, gaining access without proper credentials. See cracker.

host—A computer or network that provides services to other, linked computers on the same network. A host may supply multiple services, such as Web connectivity, ingoing or outgoing email transmission, and so on. Some definitions consider a host synonymous with a server.

host name—Not to be confused with domain name, a host name is the alphanumerical name given to a specific host computer system and part of the domain. It has a prefix, unlike the domain name. In www.xxxxx.gov, the prefix "www" means the data can be accessed via a Web browser; .gov signifies a government-based organization. Host names are much easier for humans to remember than IP (Internet Protocol) addresses, but the reverse holds true for computers.

hub—A network device where numerous connections meet.

IDS (intrusion detection system)—An automated security system that monitors network traffic, employing list-based and heuristic scanning techniques to determine whether communication should be allowed, blocked, or restricted, on an individual basis.

Internet—The sum of all interconnected public networks across the globe that are accessible using the TCP/IP Protocol.

IP (Internet Protocol)—Often seen in conjunction with the TCP (Transmission Control Protocol), as TCP/IP. While the TCP creates the communications stream between hosts, the IP determines the format of data packets. IP has been likened to addressing an envelope, which the TCP actually delivers.

IP address (Internal Protocol address)—Not to be confused with an Ethernet Address, the IP address identifies your computer, and no other computer, on a network. It's a computer's equivalent of your home telephone number, completely unique so calls can be routed your way. The address uses a protocol called IPv4 (Internet Protocol version 4), which is made up of four numbers separated by periods. All numbers are between 0 and 255, such as 216.239.51.100 (which is Google's IP address). Each successive number narrows the address location. With the burgeoning use of Web-connected electronic devices, future problems of limitation are foreseen for this system, and a new addressing scheme (IPv6) has been proposed to deal with it.

LAN (local-area network)—A data network that spans a relatively limited area, usually anywhere from a room to a couple of miles. Although larger networks are often referred to as LANs, they are more precisely called WANs (wide-area networks).

LAN topologies—A geometric arrangement of network-based devices. On a bus topology, all devices share a central cable, usually called the network backbone. A star topology has all devices connect through a central hub. A ring topology employs a closed loop, with every device connected to two others. A tree topology is a hybrid that employs clusters of star topologies linked via network backbones. Each of these configurations has its advantages and drawbacks.

line noise—Any static or electromagnetic interference on a voice or data transmission line that interferes with telephone or network communications.

login—The procedure of entering an account username and password to access a network.

malware—Any software designed with malicious intent and/or for the purpose of acquiring illicit information. Traditional examples of malware include viruses, worms, and Trojans, but spyware is malware, as well, and in some cases is eclipsing viruses and Trojans in terms of ubiquity and the severity of its potential threat.

NAT (Network Address Translation)—A means of masking IP addresses on a LAN. It provides each client host with two addresses: one used within the net, and another known outside it. The NAT simply replaces all "real" addresses with masked ones on outbound packets, and masked addresses with real ones on inbound packets. This hides the "identity" of all client hosts from the outside world. NAT can also be used to replace all network addresses with a single masked one, so that each client host has the same apparent IP address outside the network.

network—At least two computers linked to share data and/or resources (printers, Internet access, etc.)

network administrator—The person(s) responsible for the design, implementation, and management of a network.

NIC (network interface card)—The adapter card in a computer that allows it to communicate with a network. Each NIC has a unique Ethernet address.

NIS (Network Information System)—A network naming and administration system that supplies each server and host client in the system with knowledge about the entire system. As a result, a user can apply a single identification code and password to access programs on any of the LAN's hosts. Similar if not identical to the Web-based DNS. Originally created by Sun Microsystems, NIS is also available in freeware versions.

node—A computer connected to a network.

offline—Operating a computer not connected to a network, often referring to a computer that is not connected to or using the Internet.

online—Operating a computer that's part of a network.

P2P (peer-to-peer) network—Computers connected in a workgroup without a server. As the number of computers and peripherals rises, peer-to-peer networks quickly become impractical.

packet—A unit of data that starts at an originating point on a network and is sent to a destination point. Network protocols divide files into packets, or smaller, more manageable chunks of data for transmission through the TCP layer of TCP/IP. Not all the components of a single packet, sent in this way, may use the same route to a destination, since route conditions may change very quickly, and a router may switch packets to travel by alternate routes as it deems best.

packet filtering—A security measure that rejects packets from

unauthorized ports, hosts, and IP addresses.

packet sniffing—Accessing data packets traveling over a network, usually without authorization. This is typically done by crackers to acquire private passwords, credit card numbers, or simply privileged information from a network.

password—A secret series of characters that provide a particular registered user with access to network functionality.

patch panel—A device that connects computers on a LAN to one another and to all incoming and outgoing lines from another LAN, a WAN, or the Internet.

port—A connection for the direct exchange of data between two or more devices. On a network the source and destination ports are stored as special numbers (between 0 and 65535) in the header of a packet that utilizes TCP or other protocols. These numbers direct incoming data to different computer processes. Ports are vulnerable to exploits, which is why firewalls are used to stop infiltrating port scans.

PPP (Point-to-Point Protocol)—A protocol that defines the exchange of data between two computers using high-speed dial-up access on serial lines. Its most common function is to provide Internet access for computers relying upon dial-up modems. Supersedes SLIP by providing error checking and greater connection stability.

protocol—A set of conventions or rules that supply guidelines for computer communications.

proxy server—Derived from legal terminology, a server that acts as a proxy on behalf of a client. Proxy servers are frequently used as intermediaries between LANs and the Internet. They perform a variety of tasks, caching previously loaded pages to speed up access, incorporating NAT and/or firewall functionality, and more.

remote login—The ability to operate a networked computer from a remote location, using any of several protocols.

repeater—A device utilized within a network to strengthen the signal as it passes through the network cable over distances that might otherwise degrade the data signal's intensity.

router—A device that connects at least two networks. It sets the next destination point for a packet of information. Routers are located at gateways. Some routers maintain and update tables of both available network routes and their conditions, which help find the quickest path of delivery.

server—Most commonly used to describe a host computer, or one that stores shared information or that runs shared applications for connected client computers over a network. Some definitions state that a server is a software program on a host, providing services to other computers linked in a network.

SLIP (Serial Line Internet Protocol)—A protocol that defined the exchange of data between two computers using dial-up access on serial lines. It has been superseded by the Point-to-Point Protocol.

SMTP (Simple Mail Transfer Protocol)—A Web protocol used to transfer email between servers. The standard TCP/IP port used for SMTP is 25.

SNMP (Simple Network Management Protocol)—A standard protocol used on most TCP/IP networks (and some others) to monitor and manage connected devices. It collects statistics, performs specific security operations, matches configurations, and attends to a host of performance-related tasks.

switch—Sometimes called an intelligent hub, a switch checks a packet's destination information and forwards it to only a single port. On larger networks, the trip between one switch and another is called a hop, and the time it takes for the switch to send a packet is called latency. The more packets a switch has to consider each second, the greater the latency and the longer the wait before each packet moves along to its next destination point.

TCP (Transmission Control Protocol)—Often seen along with the Internet Protocol as TCP/IP. TCP allows two networked computers to form a sequenced communications stream, tracks the movement and exchange of packets, and reassembles packets into usable data correctly as they arrive at their destination.

terminator—A device used at end-points on a LAN employing a bus topology to keep the signal from reflecting back and disrupting communications.

traffic—That degree of activity that occurs on a given network over a specified period of time. It is measured through the amount of data that passes from one computer to another.

virus—Any software program that replicates itself and acts with malicious intent.

VPN (virtual private network)—A private network connecting nodes and constructed over a public system. In essence, it segregates a portion of the Web for data transmission while employing security devices so prevent unauthorized network access. In other words, a LAN within the Internet.

WAN (wide-area network)—Two or more LANs connected to one another, creating a network that covers a larger area. Often refers to networks covering states, provinces, or nations. The Internet is the largest and most obvious example of a WAN.

Wi-Fi—A wireless standard applied in WLANs to ensure compatibility among various 802.11-enabled devices.

WLAN (wireless local-area network)—A wireless LAN where connected devices communicate via radio waves on a specific frequency. Individual access stations don't require line-of-sight connection or wiring, but the backbone itself usually employs cables to a variety of centralized transmission/reception points. Many hotels and airports now employ WLANs.

workgroup—A group of nodes on a LAN that communicate and share resources and data.

What are you paying for tech support?

	Smart Computing Tech Support Center	Other On-Site Tech Support Services
Virus & Spyware Removal	FREE	$229
Set Up Wireless Network	FREE	$159
Install Operating System	FREE	$229
Install Additional Memory	FREE	$129
Install Hard Drive	FREE	$129
Operating System Service	FREE	$229
Data Migration	FREE	$229

Why pay a company to come to your home, perform these tasks, and charge you an arm and a leg for their services? The resources available at SmartComputing.com will enable you to accomplish these tasks yourself for free. Save money. Save time. And do work you can be proud of, with our help.

"In a time when customer service is hard to find, along comes Smart Computing *offering FREE tech support. This is OUTSTANDING, and you will have me as a subscriber for life."*

"Just wanted to pass along a thank you and I'm IMPRESSED! with your technical support hotline . . . Everyone was courteous and professional–I will recommend Smart Computing *to all my friends and colleagues."*

"Just wanted to let you know that I so appreciated the help I got from your staff, one who called me and guided me through to the resolution of the problem. You get an 'A' in my book. Thanks once again."

Smart Computing's Tech Support CENTER **FREE!**

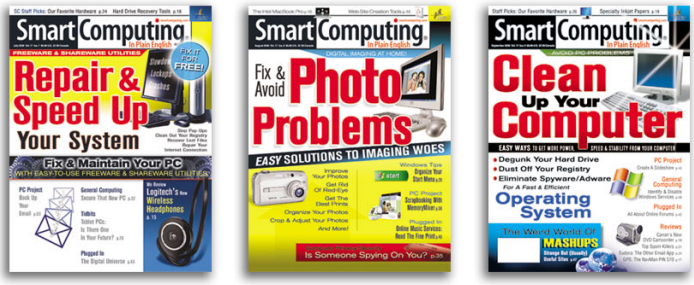
(800) 368-8304

www.smartcomputing.com/techsupport

Find answers fast … your way, the no hassle-way!

As a subscriber to *Smart Computing,* you will receive a monthly issue delivered right to your door, filled with helpful tips and troubleshooting help. Plus, subscribers receive unlimited access to SmartComputing.com, where you can find the answers fast…your way, the no hassle-way! Subscribe today to get access these helpful online tools:

- Searchable Article Archive
- Access To Current And Past Issues
- Searchable, Plain-English Dictionary
- Interactive Q&A Board
- Tech Support Center



Subscribe Today!

(800) 733-3809

SmartComputing® In Plain English smartcomputing.com

Subscriptions include unlimited access to SmartCompuitng.com!

Mention code 13565 when ordering.